GROOV BOX USER'S GUIDE FOR GROOV-AR1

GROOV BOX USER'S GUIDE

for GROOV-AR1-BASE

Form 2104-150518—May 2015

OPTO 22
Automation made simple.

Table of Contents

1: Welcome

groov is Opto 22's web-based operator interface system that is *simple*, *mobile*, and *connects easily* to almost everything.

Simple: *groov* requires only a web browser to build mobile interfaces. Because it puts ready-made gadgets at your fingertips and requires zero programming, it's simple to build, deploy, and view effective and 100% scalable operator interfaces. Using tags from a built-in Data Simulator you can test project ideas without connecting to a live machine or system.

Mobile: Get the free *groov* View app for Android or iOS for a native experience on your iPhone, iPad, or Android phone or tablet. If you have a different brand device you want to use, from a smartphone to a web-enabled big-screen TV, you can do that, too. You can view your *groov* interface on virtually any device or computer that has a modern web browser. *groov* can augment existing human-machine interfaces (HMIs) and SCADA systems by making important information available at any time and in any location. Using event notification, selected personnel can be alerted anywhere by email or a text message about system events based on multiple conditions.

Connects easily: You can connect *groov* to Modbus/TCP devices and Opto 22 SNAP PAC controllers directly, or to devices from other manufacturers through a OPC UA (Unified Architecture) server. When connected to a OPC UA server you can monitor and control PLCs and PACs such as

Allen-Bradley ControlLogix and CompactLogix, Siemens SIMATIC S7, Schneider Electric Modicon, GE PACSystems, and many more.

In addition you can use *groov* with databases, SNMP devices, weather stations, OPC-DA servers, or any device or system supported by your OPC UA server. *groov* gets important data from process control, OEM machines, and manufacturing systems into operators' hands. (For more information about OPC UA, go to opcfoundation.org/UA.)

Choose Your *groov*

groov is available as either the standalone *groov* Box hardware appliance or the PC-based *groov* Server for Windows software.

***groov* Box** (p/n GROOV-AR1-BASE) is an industrially hardened appliance that comes preloaded with *groov* software, including *groov* Build for building operator interfaces, *groov* View for using the interfaces you've built, and *groov* Admin for administering the Box itself. The *groov* Box communicates over a standard Ethernet network or wireless LAN (local area network), or both. The WiFi adapter must be purchased separately. See Appendix D: Installing an Approved USB WiFi Adapter.

***groov* Server for Windows** (p/n GROOV-SVR-WIN-BASE) includes *groov* software (*groov* Build for building operator interfaces and *groov* View for using them) and is ready for installation on a Microsoft® Windows® PC. Once installed, *groov* Server runs as a service on your computer. For more information on *groov* Server, see form 2078, the *groov Server for Windows User's Guide*.

Whether you store and serve *groov* software on a *groov* Box or on a computer using *groov* Server for Windows, an operator interface you develop with *groov* can be viewed on almost any mobile device or computer.

Internet

Modbus/TCP device

Opto 22 SNAP PAC

Assets

groov Box

Another company's automation system

groov Server for Windows

groov Build

groov View

OPC UA server (Only needed if using another company's automation system. Not needed for Opto 22 or Modbus/TCP devices.)
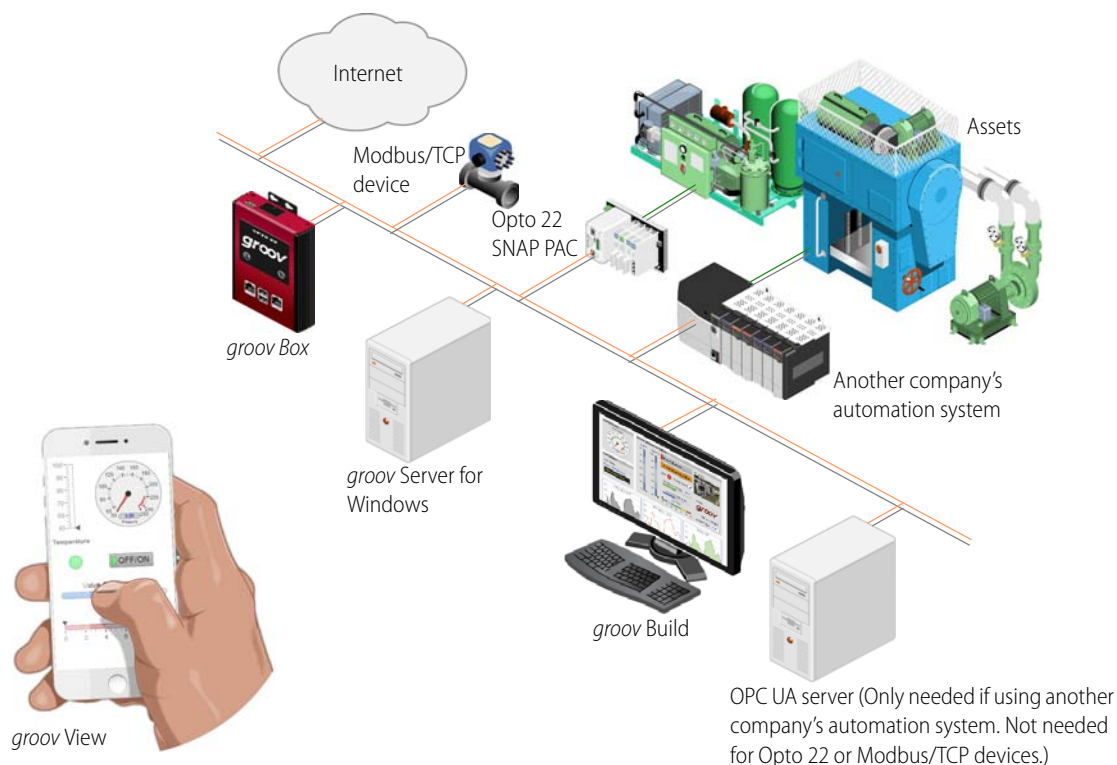
About this Guide

This user's guide shows you how to install and set up your *groov* Box, and how to use the *groov* Admin software. *groov* Admin provides the tools to back up and restore your project, update *groov*, set up wired and wireless networking, and more.

For information about building and viewing *groov* interfaces, see form 2027, the *groov User's Guide*.

Other *groov* Resources

Resources for *groov* are available on groov.com.

System Requirements

For *groov* Box

To build operator interfaces with *groov* you'll need:

- Any computer with a modern web browser. This does not have to be a Windows PC.
- One or more of the following:
    - A Modbus device that communicates over Ethernet

– An Opto 22 SNAP PAC System (SNAP PAC S-series, R-series, with firmware R9.2a or newer or SoftPAC, running a PAC Control strategy)

– Another manufacturer's automation system with tags accessible by your OPC UA server, plus the appropriate drivers for your system installed on the server computer.

A Note on Browsers

Thanks to technologies such as HTML5, SVG, and CSS3, modern browsers are now more similar than they are different. Consequently, our browser-based *groov* View and *groov* Build work reliably on a large number of device/OS/browser combinations. We've seen *groov* work on HDTVs, phones of many shapes and sizes, and new devices, and we test them as fast as we can get our hands on them. We can't test every single device/OS/browser version available. But we're happy to recommend those that work well, such as Firefox, Chrome, and Internet Explorer 10 or newer. We also encourage you to let us know your experiences with devices you find.

groov Box Communications

groov uses standard computer networks and protocols. The unit communicates with computer networks over a standard 10/100/1000 Mbps Ethernet network. For use on a wireless network, you must purchase and install a USB WiFi adapter that has been tested and approved by Opto 22. For more information, see Appendix D: Installing an Approved USB WiFi Adapter.

With two independent wired Ethernet network interfaces plus an optional independent wireless interface, the unit gives you the flexibility to monitor devices in hard-to-reach areas and to set up networking suited to your business.

In addition, you can use your *groov* Box as an access point in order to create a private wireless network with WPA2-PSK security. This is particularly useful for connecting a phone or tablet to the *groov* App when there is no other wireless network available. SoftAP can be used by any WiFi-capable device. Your *groov* Box can be connected to either a wireless or Ethernet network. See "Using an AR1 as a Wireless Access Point" on page 35.

Top

Ethernet connectors

USB connector for WiFi adapter

System Architecture

When you first set up *groov*, the PC you use must reside on the same network (broadcast domain) as the *groov* Box. In a quick and easy setup, the development PC and smartphone or tablet running View all reside within the same domain as *groov*. The controller can also be on the same network, or it can be on a separate control network as shown here. For more information, see form 1796, the *Guide to Networking Opto 22 Products*.

The following illustration shows *groov* connected to control systems from other manufacturers as well as a SNAP PAC controller. When accessing *groov* outside *groov*'s network on the Internet, a VPN (Virtual Private Network) connection is recommended for security. The Secure Sockets Layer (SSL) encrypts data exchanged between your browser and *groov*.

Assets

Control systems from other manufacturers

OPC UA server

SNAP PAC controller is recommended for running the PAC Control strategy and managing assets

groov Box

Enterprise Network

Control Network

Internet

PC running *groov* View in a modern browser

VPN server

Smartphone with View
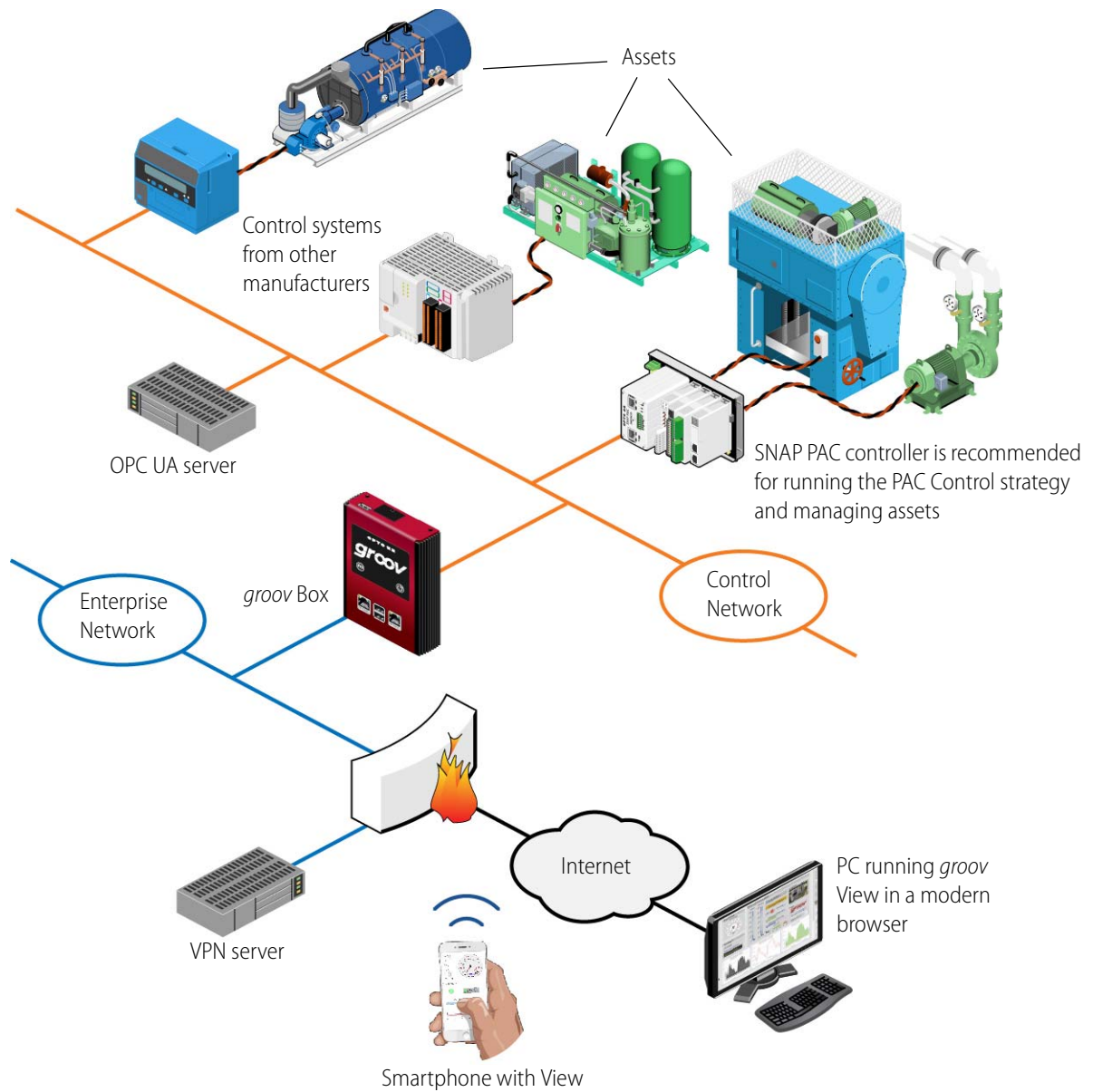
What's In This Guide

Here's what is in this user's guide:

Chapter 1: Welcome introduces this user's guide and *groov*.

Chapter 2: Getting Started describes how to get *groov* up and running quickly.

Chapter 3: Powering On, Logging In details how to log in to *groov* Build and *groov* Admin and how to manage SSL certificates.

Chapter 4: Using groov Admin describes how to use *groov* Admin to back up and restore *groov*, manage the network connections, access system information, and more.

Chapter 5: Using an SSL Certificate describes using an SSL certificate that is digitally signed either by a certificate authority (CA) or it is self-signed.

Chapter 6: Troubleshooting and Q&A provides troubleshooting information and answers questions you might have about *groov*.

Appendix A: Specifications and Dimensions provides technical specifications and *groov* Box dimensions.

Appendix B: Connectors and LEDs describes connector names and what the status and activity LEDs mean.

Appendix C: Replacing the Battery describes how to remove and replace the backup battery.

Appendix D: Installing an Approved USB WiFi Adapter provides a list of USB WiFi adapters Opto 22 has tested and approved for use with GROOV-AR1-BASE, and installation instructions.

Product Support

If you have any questions about *groov*, you can call, fax, or e-mail Opto 22 Product Support.

Phone:	800-TEK-OPTO (800-835-6786) 951-695-3080 (Hours are Monday through Friday, 7 a.m. to 5 p.m. Pacific Time)	*NOTE: Email messages and phone calls to Opto 22 Product Support are grouped together and answered in the order received.*
Fax:	951-695-3017	
Email:	support@opto22.com	
Opto 22 website:	www.opto22.com	

When calling for technical support, be prepared to provide the following information about your system to the Product Support engineer:

* *groov* Image version and *groov* Admin version. Click the System Information icon in the Admin Quick Start (see page 43).

* A description of your system equipment:

    – Computer type, speed, memory, and operating system

    – Browser type and version

    – OPC UA server type and configuration

* A description of the network

* Specific error messages or other diagnostic indications

2: Getting Started

In this chapter you'll find instructions on how to install the *groov* Box and set up the *groov* Admin software.

In this chapter:

What You Will Need

In order to set up your *groov* Box and do the activities in this chapter you will need a computer with a modern web browser on the same network you'll use for the *groov* Box. For the best user experience, we recommend Chrome, Firefox, or Internet Explorer 10 or newer.

In the Box

These items are included in the box:

• *groov Quick Start for GROOV-AR1*, form 2103

• *groov* Box (GROOV-AR1)

- *groov* CD that includes the *groov User's Guide* (form 2027), the *groov Quick Start for GROOV-AR1* (form 2103), *groov Box User's Guide for GROOV-AR1* (form 2104), and the *groov* Find utility
- Ethernet cable
- Power supply unit
- One DIN clip and one flat surface mounting bracket (includes four screws)
- Drill template for the mounting bracket
- Activation key certificate

Mounting brackets and screws

Ethernet cable

groov **Box**

CD   **Drill Template**   **Power supply**

Activation key certificate

You'll need the activation key for step 7 when you activate your groov Box, so make sure to put your activation key certificate in a safe place.

Step 1. Get To Know the *groov* Box

To set up the *groov* Box, you'll use the *groov* Box components shown below. Make sure to put the activation key certificate label in a safe place. You'll need the activation key later when you activate your *groov* Box.

SYS LED

On/Off button and Power LED

ETH0

Bottom

Power terminal

Step 2. Choose a Location

When deciding where to place the groov Box, make sure there is room around the front, top, and sides of the groov Box to allow air to flow freely around the device. You need to be able to see the information on the bottom. Also see .

Step 3. Mount the *groov* Box

Mounting brackets are provided for you to attach the *groov* Box to a flat surface or a DIN rail. If there will be vibration at the *groov* Box installation site, make sure to mount the device to a flat surface for a secure installation.

For mounting on a flat surface:

a. Using the screws provided, install the surface mounting bracket on the back of the *groov* Box.

Surface mounting bracket

b. Using the hole template provided, drill holes for #6 or #8 screws in the mounting surface.
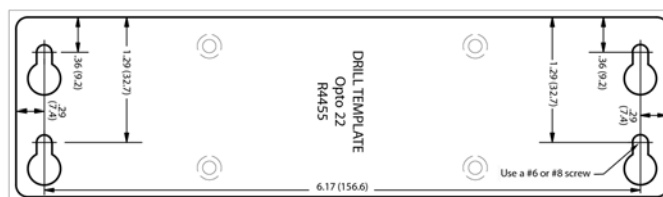
c. Secure the device to a flat surface with #6 or #8 screws.

For mounting on a DIN rail:

a.   Using the screws provided, install the DIN rail clip on the back of the *groov* Box.

DIN rail clip

b.   Attach the *groov* Box to the DIN rail.

Step 4. Connect to the Network

ETH1 to control network
(if on a separate subnet)

ETH0 to computer network
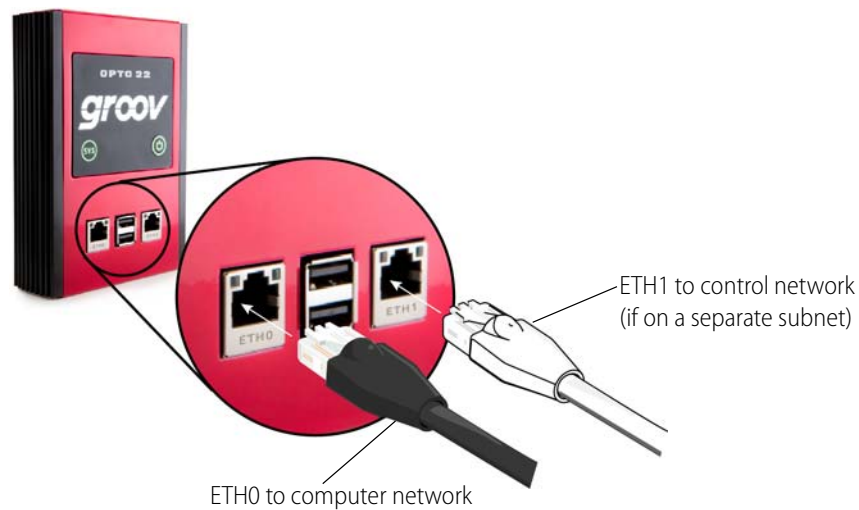
a.   Connect an Ethernet cable from ETH0 to your computer's network.

NOTE: Opto 22 recommends connecting ETH0 to a network with DHCP and DNS services. If you do not have these services, you'll need to manually configure networking.

b.   The two independent Ethernet connectors (ETH0 and ETH1) have separate IP addresses that can be used to segment a control system's network from the enterprise LAN. If your Opto 22

controller, OPC UA server, or Modbus device is on a different network than your computer, connect ETH0 to your computer's network and ETH1 to the other network.

If you are using both ETH0 and ETH1, make sure they have IP addresses on different subnets. In some situations, this may require configuring a static IP address. Otherwise there may be communication errors. For more information, see "Assigning a Static IP Address" on page 29.

For detailed information on setting up your network and setting up communications over the Internet, see form 1796, the *Guide to Networking Opto 22 Products.*

Step 5. Connect the Power Supply

Your *groov* Box requires a power supply with an output of 8–36 VDC, 24 VDC @ 500 mA. You can use the power supply that comes with the *groov* Box, or provide your own. In either case, we recommend using a UPS (uninterruptible power supply) for backup power and surge protection.

If you are using the power supply that came with the *groov* Box, do the following:

Plug the small connector on the power supply into the power terminal on the bottom of the *groov* Box, and tighten the screws. Plug the other end into a standard 120 or 240 VAC outlet.

If you are using your own power supply, do the following:

a. With the power supply off or unplugged, connect the + (positive) lead from the power supply (normally red) to the + (positive) terminal on the power connector.

CAUTION: Reversing wire polarity may cause damage to your groov Box. This damage is not covered by Opto 22's warranty. If you are not certain about the polarity of the wires on your power supply, check with a meter.

b. Connect the COM wire from the power supply (normally black) to the – (negative) terminal on the power connector.

c. Plug the power supply into a standard 120 or 240 VAC outlet.

Step 6. Turn on the *groov* Box

Firmly press the On/Off button until the SYS LED lights up (in about one second), then release. Take a look at the LNK ACT light for ETH0; if the cable is properly connected, the LNK ACT light should be on or blinking.

On/Off button and Power LED

ETH0 LNK ACT light

NOTE: Always wait until the SYS LED has stopped blinking before you try to log into groov. Otherwise, you may not be able to use the hostname to log in. If this happens, see page page 65.

***CAUTION**: If you press the button for longer than eight seconds, the groov Box will be reset to default settings. Your project and all passwords will be erased.*

Step 7. Activate the *groov* Box and Get the License File

a. Open a web browser. Go to activate.groov.com.
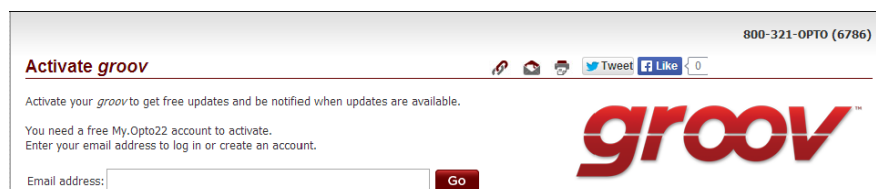
b. Log in using your email address and your My.Opto22 password.

You may have set up your free My.Opto22 account when you purchased your *groov* Box. If you don't have a My.Opto22 account, enter your email address and other information, and the account will be created.

c. Follow the on-screen instructions to activate your *groov* Box and download the license file.

The activation key is printed on the activation key certificate included with the *groov* Box. When asked to enter the serial number, you'll find it on the label on the bottom of the device.

Serial number
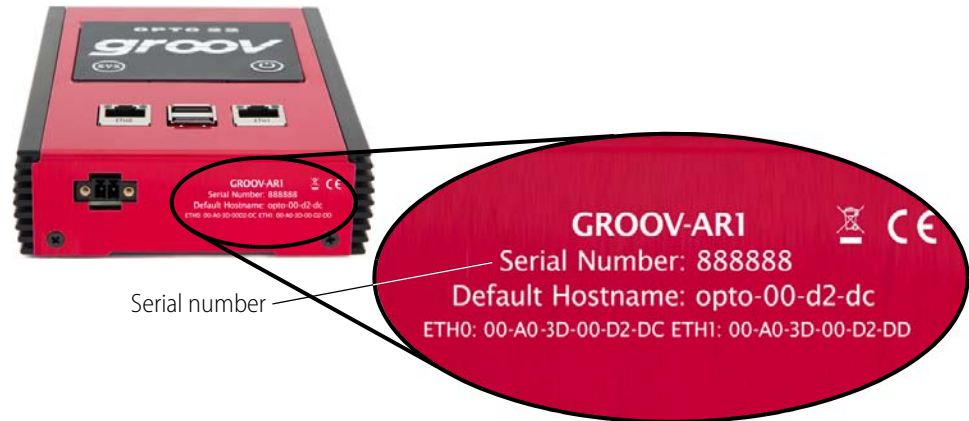
d. After activating the *groov* Box and downloading the license file, return to this guide and continue with step 8.

Step 8. Open *groov*

You can open *groov* using just your web browser. Or, if you have a Windows computer, you can use *groov* Find (see below). If your network does not have DNS, use *groov* Find.

Using your web browser:
a. Make sure the SYS LED on the *groov* Box has stopped blinking.
b. On your computer, open Firefox, Chrome, or Internet Explorer 10.
c. Enter https:// and your *groov* Box's hostname as the URL. The hostname is printed on the bottom of the *groov* Box.

For example, if the hostname is opto-00-d2-dc, you type
`https://opto-00-d2-dc`

Hostname

Make sure you type http**s**. The **s** indicates it is a secure connection.

NOTE: If you've assigned a static IP address to the groov Box, or if your network doesn't provide DHCP and DNS services, use the IP address instead of the hostname to open groov.

d. Accept the security warning as described below. For more information, see "Accepting the Security Warning" on page 23.

For Chrome:

– Click "Advanced" to expand the initial screen.

– Click "Proceed to *<hostname>* (unsafe)."

For Firefox:

– Expand "I Understand the Risks."

– Click Add Exception to open the Add Security Exception dialog box.

– Select "Permanently store this exception."

– Click Confirm Security Exception.

For Internet Explorer 10 or newer: Click "Continue to this website (not recommended)."

For Safari: Click Continue.

The **Welcome to *groov*** window opens in your web browser. Now go to "Step 10. Install the License File" on page 18.

Using *groov* Find:

If you are using a Windows computer, you can use *groov* Find to locate the *groov* Box on your network.

a. Insert the *groov* CD in your CD-ROM drive, then click the link to copy the Find application file to your computer. *groov* Find can also be downloaded from groov. com or the Opto 22 website.

b. Open the Find application file.

A message might appear asking if you want Find to be allowed to make changes to your computer. If it does, click Yes.

NOTE: If you are using a Windows account that does not have Administrator privileges (such as Guest), a User Account Control dialog box will appear asking for the credentials of an administrator account. To proceed, enter the Administrator User Name and Password. If you do not have this information, contact your IT department.

groov Find opens and automatically searches for *groov* Boxes on the network.

c. Find the serial number on the bottom of the *groov* Box.
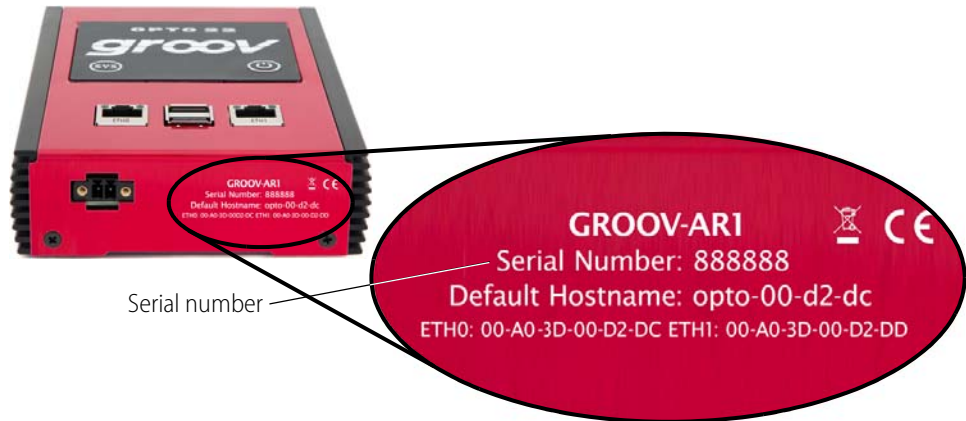
Serial number

d. Locate the matching serial number in Find.
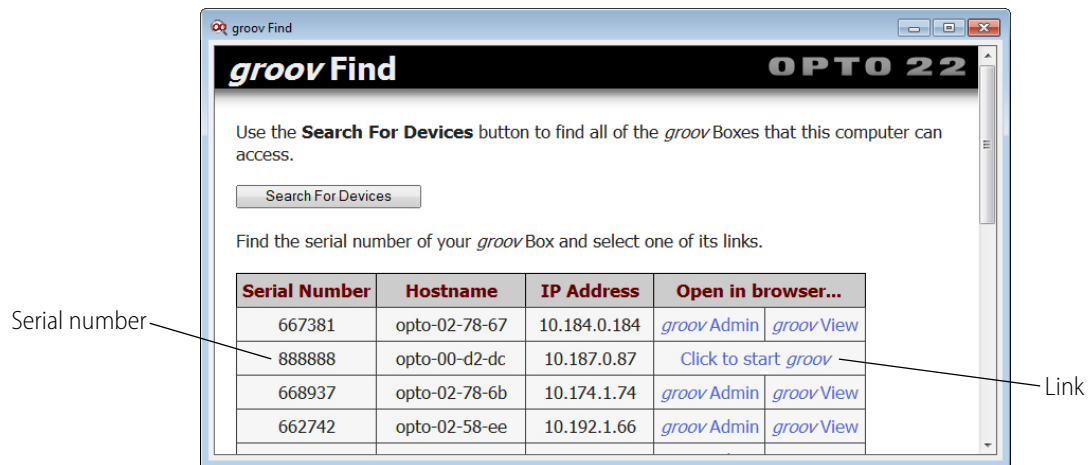
Serial number

Link

If you do not see the serial number right away, wait 60 seconds and click Search for Devices again.

e. Click the link "Click to start *groov*."

When your browser connects to *groov* for the first time, the browser will display a *security warning*. This is normal behavior for *groov*.

f. Accept the security warning as described below. For more information, see "Accepting the Security Warning" on page 23.

 For Chrome: Click "Proceed anyway."

 For Firefox:

– Expand "I Understand the Risks."

– Click Add Exception to open the Add Security Exception dialog box.

– Select "Permanently store this exception."

– Click Confirm Security Exception.

For Internet Explorer 10 or newer:
Click "Continue to this website (not recommended)."

For Safari: Click Continue.

The **Welcome to *groov*** window opens in your web browser.

Step 9. Create a *groov* Admin Account

Follow the on-screen instructions to create a username and password for *groov* Admin. The Admin account is for administrative tasks such as changing or editing the network connections and updating the *groov* Box.

CAUTION: *Write down your Username and Password, and keep them in a safe place. You will need this information each time you log in. If you lose your login information, you will have to reset the groov Box to factory defaults, which will erase your project. There is no password recovery option.*

Step 10. Install the License File

Make sure to install your license file. Without an installed license, *groov* will only work for two hours.

a. When prompted to add a license file to *groov*, click Install License.

groov

You're almost ready!

Your *groov* Box is unlicensed. Without a license file, *groov*'s capabilities are limited.

License *groov* now

Install License...   If you don't have the license file, click here for instructions.

Use *groov* in Trial Mode

If you don't want to add a license right now, you can run *groov* in Trial Mode. *groov* Build will be fully functional, but *groov* View will be limited to two hours.

Start Trial Mode

b. Browse to the license file, then click Open.

Your license is now installed.

Step 11. Create a *groov* Build Account

A Build account lets you create and edit a project in *groov* Build.

a. When prompted, enter a new username and password. Enter the password again to confirm.

b. Click Create *groov* Build Account.

c. Click Go to *groov* Build. *groov* Build opens in your browser.

If you have any trouble opening *groov*, see Troubleshooting in form 2027, the *groov User's Guide*.

3: Powering On, Logging In

In this chapter:

Before using the information in this chapter, install your *groov* Box and set it up on the network. For instructions, see Chapter 2: Getting Started.

Using the On/Off Button

The On/Off button can do the following:

- Turn the *groov* Box on and off.

- Reset the *groov* Box to the factory state

SYS LED ————— (SYS)   (⏻) ————— On/Off button/
                                    Power LED

Turning On the *groov* Box

1. Check to make sure that the *groov* Box is plugged in and receiving power.
2. Firmly press the On/Off button until the SYS LED lights up (in about one second), then release.

    Take a look at the LNK ACT light for ETH0; if the cable is properly connected, the LNK ACT light should be on or blinking.

    NOTE: Always wait until the SYS LED has stopped blinking before you try to log into groov. Otherwise, you may not be able to use the hostname to log in. If this happens, see page 65.

    ***CAUTION**: If you press the button for longer than eight seconds, the groov Box will be reset to default settings. Your project and all passwords will be erased.*

Turning Off the *groov* Box

With the *groov* Box on, press the On/Off button. The SYS LED will blink blue and then turn off. Always allow the *groov* Box to turn off properly before removing power.

Resetting *groov* Box to the Factory State

Resetting the *groov* Box resets the default network settings and erases all user data, including your project. *groov* will be in the state it was when shipped from the factory, so any upgrade to *groov* Admin, *groov* App, or license(s) will have to be re-applied.

***CAUTION**: When the groov Box is reset to factory default settings, your project and all passwords will be erased.*

1. Check to make sure that the *groov* Box is turned off, but the device is plugged in and receiving power.
2. Press and hold the On/Off button for at least eight seconds and until the SYS LED is blinking red and green. Then release the button.

    The reset defaults operation can last several minutes. When the process is complete, the *groov* Box will power off.

    NOTE: Do not remove power from the groov Box or turn it off while the SYS LED is blinking red and green. If you do, you'll need to repeat the reset defaults operation from step 1.

3. Firmly press and release the On/Off button to turn on the *groov* Box.

    NOTE: Always wait until the SYS LED has stopped blinking before you try to log into groov. Otherwise, you may not be able to use the hostname to log in. If this happens, see page 65.

Opening Admin

Using *groov* Admin you can back up and restore your projects and project settings, update firmware, set up wired and wireless networking, and more.

To open *groov* Admin, you need to know the default hostname, which is printed on the bottom of the *groov* Box. If you want to change the hostname, see "Changing the Hostname, DNS Servers, or IPv4 Gateway" on page 30. To use Admin, see Chapter 4: Using groov Admin.

To open *groov* Admin using a URL:

In your web browser, enter https://*hostname*:10000

For example:

```
https://opto-00-d2-dc:10000/
```

hostname   port 10000

Hostname

To open *groov* Admin using *groov* Find (Windows only)

groov Find is a utility included on the *groov* CD that locates your *groov* Box on the network and provides a link so that you can access the *groov* applications. It is especially useful if you have multiple *groov* Boxes because it finds and lists them all.

1. Open *groov* Find.

    If you have User Account Control (UAC) turned on, a message appears asking if you want Find to be allowed to make changes to your computer.
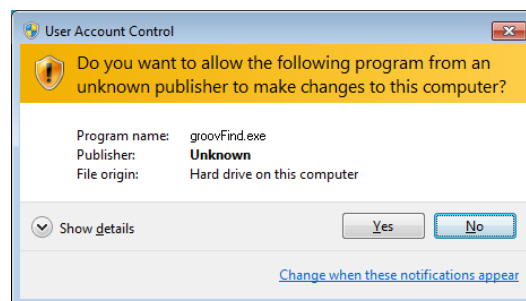
NOTE: If you are using a Windows account that does not have Administrator privileges (such as Guest), you will need to enter the Administrator User Name and Password in order to use groov Find. If you do not have this information, contact your IT department.

2. Click Yes.

NOTE: Clicking Yes permits Find to have temporary administrative privileges to create an additional temporary link-local IP address for each network interface on the computer. This enables Find to locate a groov Box on a network that does not have DNS and DHCP.

If the network does not have DNS and DHCP, you will need to assign a static IP address to the groov Box in order to maintain communication. (See "Assigning a Static IP Address" on page 29.) If the network does have DNS and DHCP, the temporary IP address is not used and is removed when you exit Find.

groov Find opens and automatically searches for *groov* Boxes on the network.

3. Find the serial number on the bottom of the *groov* Box.

Serial number

GROOV-AR1
Serial Number: 888888
Default Hostname: opto-00-d2-dc
ETH0: 00-A0-3D-00-D2-DC ETH1: 00-A0-3D-00-D2-DD

4. Locate the matching serial number in Find.

Serial number

Link

Serial Number	Hostname	IP Address	Open in browser...	
667381	opto-02-78-67	10.184.0.184	*groov* Admin	*groov* View
888888	opto-00-d2-dc	10.187.0.87	Click to start *groov*	
668937	opto-02-78-6b	10.174.1.74	*groov* Admin	*groov* View
662742	opto-02-58-ee	10.192.1.66	*groov* Admin	*groov* View
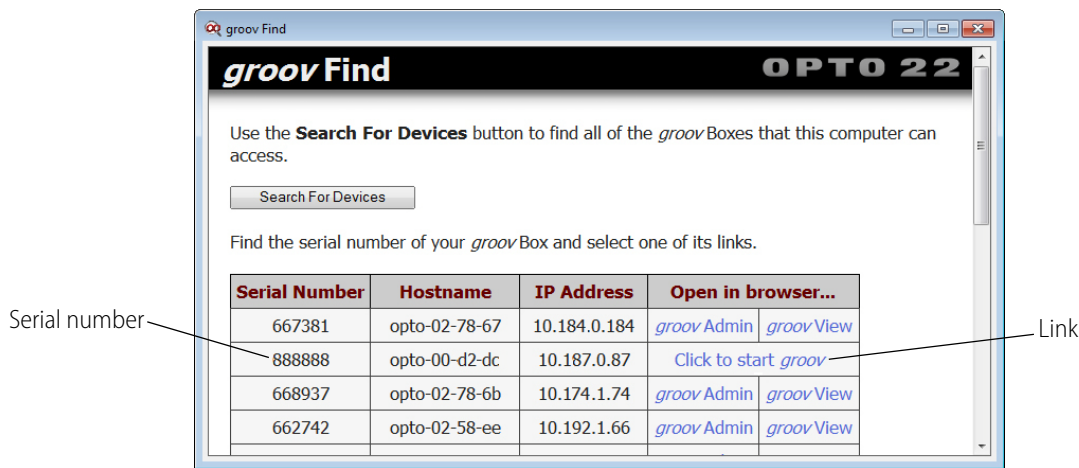
5. Click the link "Click to start *groov*."

A security warning appears in your web browser.

6. Dismiss the security warning. For more information, see "Accepting the Security Warning" on page 23.

The **Welcome to *groov*** window opens in your web browser.

If you have already created a new user and password in *groov* Admin, the *groov* Admin and *groov* View links will be available instead. In that case, click *groov* Admin.
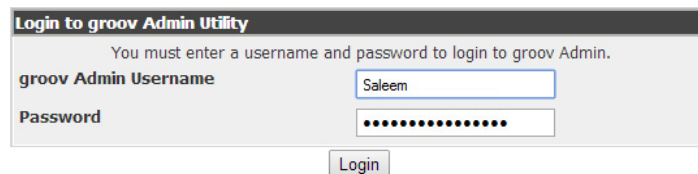
Next see (below).

Logging into Admin

CAUTION*: **There is no password recovery option**. Write down your Username and Password, and keep it in a safe place. You will need this information each time you log in. If you lose your login information, you will have to reset the groov Box back to factory defaults which will erase your project.*

To log in:

1. Enter the *groov* Admin account Username and Password.

Login to groov Admin Utility
You must enter a username and password to login to groov Admin.

groov Admin Username	Saleem
Password	••••••••••••••••

Login

2. Click the Login button.

groov Admin appears.

NOTE: There is a session timer of 10 minutes. If you don't do anything for 10 minutes, you will be logged out and have to log in again.

Accepting the Security Warning

groov uses the Secure Sockets Layer (SSL) to protect your data by encrypting data exchanged between your browser and the *groov* Box. When a device attempts to access *groov*, your browser will issue a security warning unless the appropriate SSL security certificate is installed on the device.

If your computer resides in the same domain as the *groov* Box, you can safely accept the warning because your data is protected by SSL's 256-bit encryption. However, if you want to avoid seeing the security warning, you can install the self-signed certificate on your computer and other devices that access *groov*. See .

If your computer or other device will access *groov* applications from outside *groov*'s network or over the Internet, Opto 22 strongly recommends you obtain an SSL Certificate from a third-party company that is authorized to confirm your user's ID. See .

To accept the security warning, see one of these sections:

-
-
-
-

For Chrome

– Click "Advanced" to expand the initial screen.

passwords, messages, or credit cards).

Advanced

Back to safety

– Click "Proceed to <*hostname*> (unsafe)."

information, or an attacker may be trying to intercept your communi
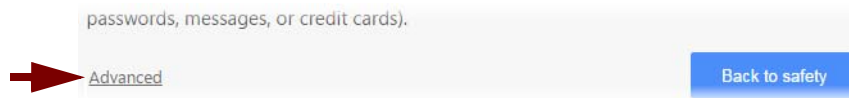
Proceed to groov-scara (unsafe)
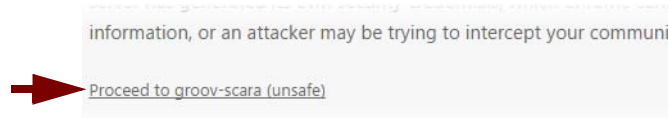
For Firefox

1. Expand "I Understand the Risks."
2. Click Add Exception to open the Add Security Exception dialog box.
3. Select Permanently store this exception.
4. Click Confirm Security Exception.

This Connection is Untrusted

You have asked Firefox to connect securely to **10.158.0.158:8443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site w
impersonate the site, and you shou

Get me out of here!

▶ **Technical Details**

Expand this ——— ▶ **I Understand the Risks**

If you understand what's going on,
you trust the site, this error coul

Don't add an exception unless you
identification.

Click here——— Add Exception...

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.158.0.158:8443/   Get Certificate

Certificate Status

This site attempts to identify itself with invalid information.   View...

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

Click here———   Confirm Security Exception   Cancel

For Safari

Click Continue.

Click here ——

For Internet Explorer

Click "Continue to this website (not recommended)."

Click here ——
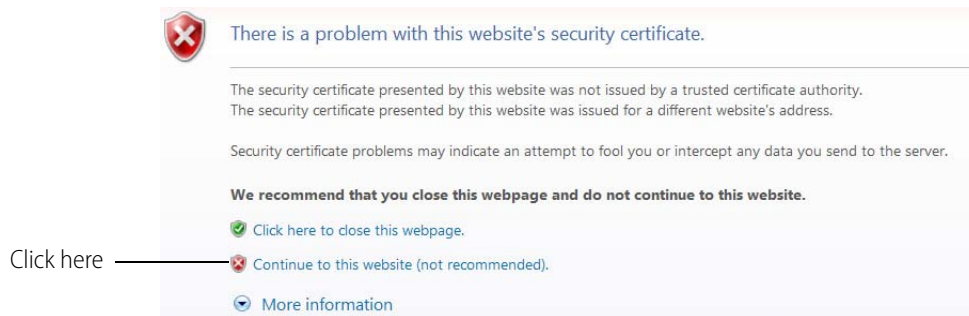
Opening *groov* App (*groov* Build and View)

Click *groov* App in the menu tree on the left side of the screen. For information on how to use *groov* Build and View, see form 2027, the *groov* User's Guide.
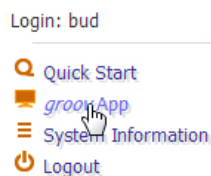
4: Using *groov* Admin

Using *groov* Admin you can back up and restore your projects and project settings, update firmware, set up wired and wireless networking, and more.

In this chapter:

To open *groov* Admin:

In your web browser, enter https://*hostname*:10000

For example:

```
https://opto-00-d2-dc:10000/
```

                  hostname   port 10000

To open *groov* Admin using *groov* Find:

In *groov* Find, locate the your *groov* Box's serial number, and click the *groov* Admin link.

Using Admin's Quick Start

Admin's Quick Start links to system settings that may need configuration out of the box. You can access Quick Start by clicking on Quick Start in the Admin menu tree.
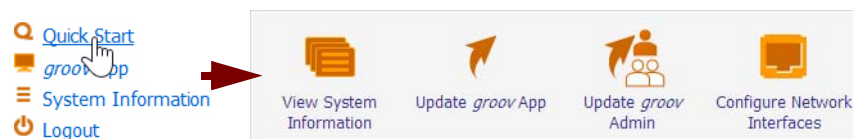
View System Information
Check system information and see usage statistics. "Checking System Information" on page 43.

Update *groov* App
Update *groov* Build and View. See "Updating groov App (Build and View)" on page 36.

Update *groov* Admin
Update your entire *groov* Admin installation to a new version. See "Updating groov Admin" on page 40.

Configure Network Interfaces
Configure IP settings for the wired and optional wireless Ethernet interfaces: ETH0, ETH1, and WLAN0. See "Configuring Network Connections" on page 28.

Configuring Network Connections

groov is designed to work with a network that has a Dynamic Host Configuration Protocol (DHCP) server and a Domain Name Server (DNS). In this case, you do not need to assign an IP address to the *groov* Box; you just plug it in and the IP address is assigned automatically. This is the recommended method for setting up the *groov* box. However, if you need to customize your network connections for *groov* after the initial setup, *groov* Admin provides the tools to do that.

This section includes the following topics:

- "Assigning a Static IP Address" on page 29
- "Changing the Hostname, DNS Servers, or IPv4 Gateway" on page 30

- "Configuring ETH1 for the Control Network" on page 31
- "Configuring Wireless Communications" on page 32
- "Using an AR1 as a Wireless Access Point" on page 35

If you need information on how to set up your network, see form 1796, the *Guide to Networking Opto 22 Products*. This guide provides detailed information on how to make your *groov* network more secure by separating control network traffic from the computer network. It also describes how to directly communicate with *groov* over the Internet using a virtual private network (VPN) or with port forwarding (PF). While PF is easier to set up, a VPN is recommended because it is more secure.

Assigning a Static IP Address

If you do not have a DHCP server, you'll need to configure a static address to either ETH0 or ETH1. Otherwise there may be communication errors.

NOTE: If you are using a laptop computer to assign an IP address, make sure you disable Windows' Internet Connection Sharing (ICS). If you don't, the laptop will act like a DHCP server and assign a dynamic address.

You'll need to get the following networking information from your IT department:

- **IPv4 address**—A unique, fixed (static) IP address.

  For example: 172.18.234.1

- **Netmask**—Identifies the subnetwork.

  For example: 255.255.225.0

- **Gateway** (optional)— Identifies the route to the Internet.

  For example: 172.18.1.1

1. Click the Configure Network Interfaces icon in Quick Start.

2. Click the wired Ethernet connection you want to configure.

   NOTE: Use ETH0 as the main network connection. Only use ETH1 if you have segmented networks.

Network Configuration

To edit an Ethernet interface, click on the name.

Name	Type	MAC Address	IPv4 Address	Netmask	IP Configuration	Link Status
ETH0	Ethernet	00:A0:3D:00:D2:DC	10.192.1.48	255.255.192.0	From DHCP	Up
ETH1	Ethernet	00:A0:3D:00:D2:DD	None	None	From DHCP	Down
WLAN0	Wireless Ethernet	Unknown	None	None	Disabled	

Edit ETH0 Interface

Boot Time Interface Parameters

Name	ETH0
IPv4 Address	○ **Disabled**
	○ **From DHCP**
	◉ **Static configuration** IPv4 Address [ ] — Static IP address
	Netmask [ ]

3. Select Static configuration and enter a static IP address and Netmask.

4. Click Save.

Changing the Hostname, DNS Servers, or IPv4 Gateway

In order to identify the *groov* Box more easily on the network, you might want to change the hostname from the default. And, depending on your network setup, you might need to change the DNS Servers or IPv4 Gateway.

NOTE: Keep in mind that any changes to this interface may make your system inaccessible via your current wired or wireless connection. Be sure to write down the new hostname or any other changes.

1. Click the Configure Network Interfaces icon in Quick Start.

Configure Network
Interfaces

2. In the Client Options dialog box, change the hostname, DNS servers, or IPv4 Gateway as necessary.

NOTE 1: A hostname cannot have spaces or special characters.

NOTE 2: Any changes to this interface may make your system inaccessible via your current wired or wireless connection. Be sure to write down the new hostname or any other changes.

3. Click Save.

Configuring ETH1 for the Control Network

If your computer is on a different network than the control network, you need to configure ETH1 by assigning it an IP address and subnet appropriate for the control network.

1. Click the Configure Network Interfaces icon in Quick Start.

2. Click ETH1.

3. If the network has DNS and DHCP, select "From DHCP." If it doesn't, enter a static IP address and Netmask.

NOTE: If you are using static addresses, ETH1 must be on a different subnet than ETH0.

4. Click Save.

Configuring Wireless Communications

If you want to use your *groov* Box on a wireless network, you must purchase and install a USB WiFi adapter that has been tested and approved by Opto 22. See Appendix D: Installing an Approved USB WiFi Adapter.

You can configure the *groov* Box to connect to a wireless network through an access point using the 802.11b, 802.11g, and 802.11n protocols.

Before you begin, get the following information from your IT Department:

SSID—Name of the wireless network access point you want the *groov* Box to join

Security—Encryption type (WPA or WPA2), network key input type (hex or ASCII), and password

Password—To access the wireless network

1. With the *groov* Box connected via ETH0, click the Configure Network Interfaces icon in Quick Start.

2. Click WLAN0.

Network Configuration

To edit an Ethernet interface, click on the name.

Name	Type	MAC Address	IPv4 Address	Netmask
ETH0	Ethernet	00:A0:3D:00:D2:DC	10.192.1.48	255.255.192.0
ETH1	Ethernet	00:A0:3D:00:D2:DD	None	None
WLAN0	Wireless Ethernet	Unknown	None	None

Edit WLAN0 Interface

Enter Wireless Network Information

Network Name (SSID)	
Encryption Type	None
Network Key Type	ASCII/Passphrase
Network Key	

3. Enter the Network Name (SSID)

The SSID is a text string from 1 to 32 characters used to uniquely identify the wireless network. This should match the SSID of the access point you want to connect to.

NOTE: If the SSID contains one or more spaces, enclose the SSID with quotation marks. For example, enter "Opto 22" instead of Opto 22.

4. Select the Encryption Type.

This is the type of encryption used to encrypt any packet sent or received between the access point and the *groov* Box.

– **None**—No encryption used.

– **WEP64**—Use WEP encryption with a 5 digit ASCII or 10 digit hexadecimal key. WEP has been deprecated by IEEE and should not be used in new installations.

– **WEP128**—Use WEP encryption with a 13 digit ASCII or 26 digit hexadecimal key.

NOTE: WEP is not secure and has been deprecated by the Institute of Electrical and Electronics Engineers (IEEE). Do not use WEP in new installations unless it is the only option available. Use WPA or WPA2 instead.

– **WPA**—Use TKIP encryption (RC4) with an 8 to 63 digit ASCII or 64 digit hexadecimal key.

– **WPA2**—Use CCMP encryption (AES) with an 8 to 63 digit ASCII or 64 digit hexadecimal key.

5. Choose the Network Key Type.

Select ASCII or Hexadecimal keys. Typically, WEP uses hexadecimal keys and WPA uses ASCII keys.

6. Enter the Network Key.

Use the key for the Encryption Type selected above. This is a write-only field.

7. In the Boot Time Interface Parameters, select From DHCP.

Normally, the DHCP server assigns an IP address. However, if no DHCP server is present, a static IP address may be used.

8. Click Save.

Wait till you see the following message.

Congratulations. You're connected!

9. If ETH0 and WLAN are on the same subnet, disconnect the cable from ETH0.

NOTE: You need to disable ETH0 because groov Box will continue to communicate over ETH0 as long as it is connected on the same subnet and enabled. However, if you are using a control network and enterprise network, and ETH0 is on a different subnet, you can leave it connected.

10. Disable ETH0 as follows:
   a. Click ETH0.
   b. Select Disabled, then click Save.

   c. Click the Back button, and notice that ETH0 is disabled (Down) and WLAN0 is now enabled (Up).

Name	Type	MAC Address	IPv4 Address	Netmask	IP Configuration	Link Status
ETH0	Ethernet	00:20:0C:30:B6:5A	None	None	From DHCP	Down
ETH1	Ethernet	00:A0:3D:02:2A:A6	None	None	From DHCP	Down
WLAN0	Wireless Ethernet	00:26:C7:22:A6:A6	None	None	From DHCP	Up

Using an AR1 as a Wireless Access Point

groov's SoftAP (Software Access Point) feature allows you to use your *groov* Box as an access point in order to create a private wireless network with WPA2-PSK security. This is particularly useful for connecting a phone or tablet to the *groov* App when there is no other wireless network available. SoftAP can be used by any WiFi-capable device. Your *groov* Box can be connected to either a wireless or Ethernet network.

In order to use SoftAP, you will need one of the following WiFi adapters:

- Netis WF2119S

- Netis WF2116

These are the *only* WiFi adapters tested and approved for this feature.

1. Follow the instructions on page 73 to install your Netis WF2119S USB WiFi adapter.

2. With the *groov* Box connected via ETH0, click the Configure Network Interfaces icon in Quick Start.

3. Click WLAN0, and make sure that WLAN0 is Disabled. (To disable it, select Disabled next to IPv4 Address in the Boot Time Interface Parameters dialog box.)

Make sure that WLAN0 is Disabled

4. Click the Wireless Access Point tab.

5. Next to **Enable?**, choose Yes to enable this feature.

6. Edit the following parameters as necessary:

   – **Static IPv4 Address**—Use an IP address that is not on the same subnet as ETH0 or ETH1.

– **Network Name (SSID)**—Enter a name between 1 and 32 characters.

– **Network Key**—Enter a key between 8 and 63 characters.

– **Channel**—The WiFi Channel should be between 1 and 14, depending on the geographic region. Click *Execute WiFi Sight Survey* to display a table of detectable WiFi access points and populate the Channel field with the quietest channel available.

7. Click Save.

Now you're ready to connect your wireless device to your new wireless network using the Network Name and Network Key. For information about using a mobile device with *groov*, see form 2105, the *Setting Up groov Mobile Apps Technical Note*.

Updating *groov* App (Build and View)

1. Back up your project before updating *groov*.

2. Make sure the *groov* Box is activated. See "Step 7. Activate the groov Box and Get the License File" on page 14.

3. Go to manage.groov.com and follow directions to download the latest *groov* update file.

4. Open *groov* Admin.

5. Click Quick Start and then the Update *groov* App button.
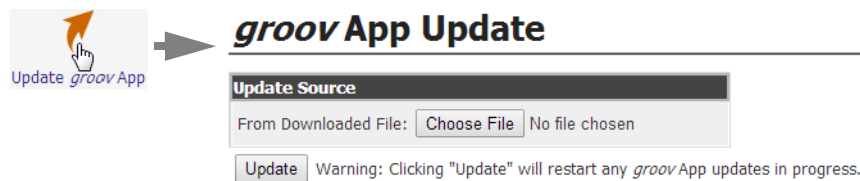
6. Click Choose File, find the downloaded update file, and then click Open.

7. Click Update.

The application is installed and restarted automatically. When the operation is complete, a success message appears.

Backing Up *groov*

During backup, project components are saved to a file on your computer or a USB flash drive. You should back up *groov* frequently. There is no automatic backup.

To restore *groov* from the backup file, see "Restoring groov" on page 39.

IMPORTANT: Your groov project files are not encrypted or obfuscated in any way. This means that most of the project information in them (except for the groov User passwords) can be read, including the following:

- *SMTP account info (including password)*
- *User email accounts (does not include the groov User passwords, which are securely hashed before being stored)*
- *Device addresses*
- *Tag address information (PAC tag names, Modbus addresses, OPC node-id, etc.)*

Opto 22 recommends that you secure your backup files using file or disk-based encryption provided either by the operating system or other software/hardware.

Also, be aware that if you send project files to Opto 22, our personnel will have access to the information listed above.

Follow these steps to back up groov:

1. In the Admin menu tree, click System, and then click Backup and Restore.
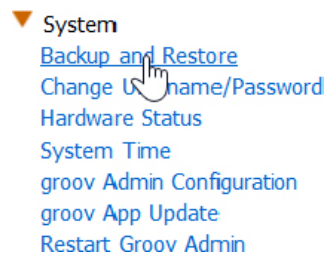
2. Select the Backup tab.

3. Select the components you want to back up.

groov **(Build, View, projects)** saves your *groov* App (Build and View) and your project.

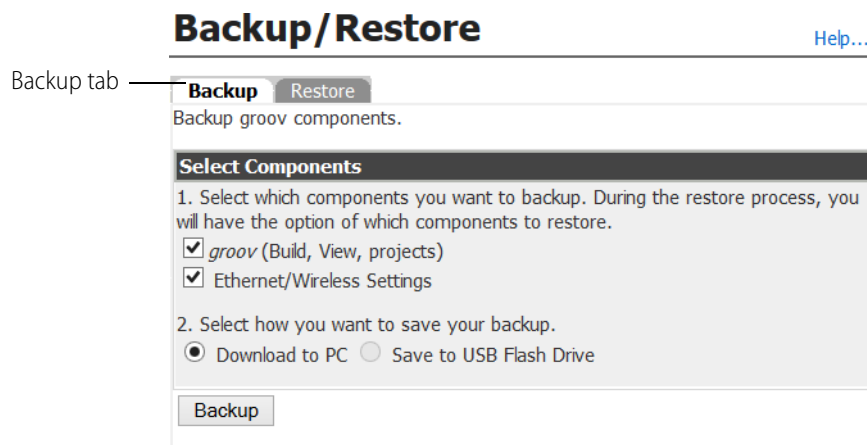**Ethernet/Wireless Settings** saves any settings configured for ETH0, ETH1, and the wireless network. This includes IP, Subnet, Gateway, Hostname, SSID, Wireless Network Key, etc.

4. Do one of the following:
   – Select Download to PC.
   – Insert a USB drive into a USB slot on the front of the *groov* Box. Then select Save to USB Flash Drive.

USB connectors for backing up and restoring

5. Click Backup.
6. If saving to the PC, select Save File in the dialog box that appears, then click OK. The backup file is downloaded to the Downloads directory on your PC.
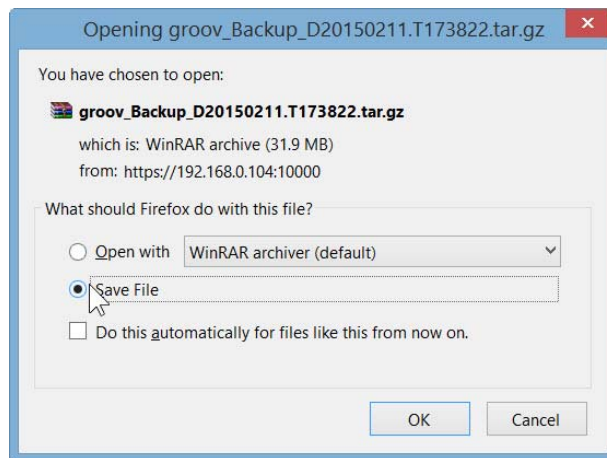
If saving to a USB flash drive, the file downloads to your USB drive.

Backup/Restore

Executing backup of groov to USB Flash drive...

Restoring *groov*

Use the following instructions to restore *groov* components from a backup file saved on a computer or USB flash drive.

1. In the menu tree, click System, and then click Backup and Restore.

▼ System
Backup and Restore
Change Username/Password
Hardware Status
System Time
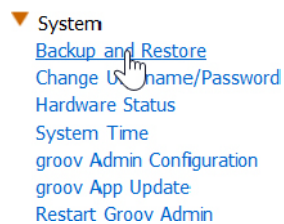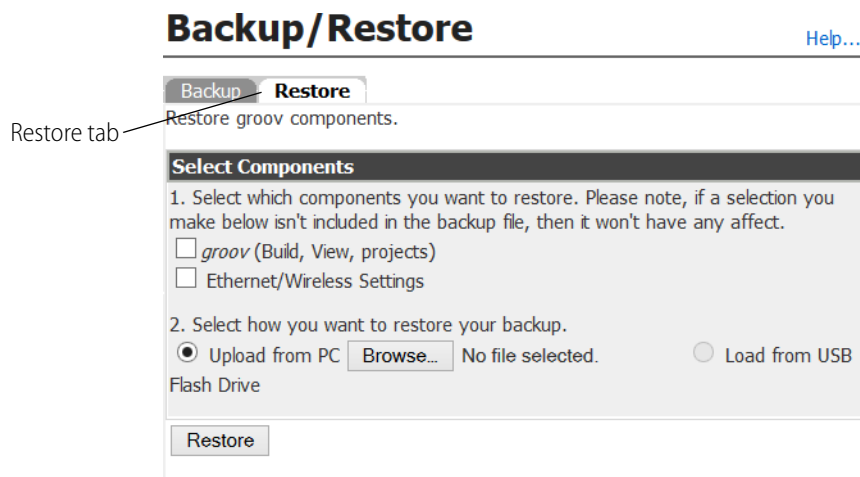groov Admin Configuration
groov App Update
Restart Groov Admin

2. Select the Restore tab.

Backup/Restore   Help...

Backup **Restore**
Restore groov components.

Restore tab ——

Select Components
1. Select which components you want to restore. Please note, if a selection you make below isn't included in the backup file, then it won't have any affect.
☐ *groov* (Build, View, projects)
☐ Ethernet/Wireless Settings

2. Select how you want to restore your backup.
◉ Upload from PC Browse... No file selected.   ○ Load from USB Flash Drive

Restore

3. Select the components you want to restore. Please note, if a selection you make below isn't included in the backup file, then it won't have any affect.

groov (Build, View, projects) restores the *groov* software and the projects you've built in *groov*.

4. Do one of the following:

– To restore from your PC, select Upload from PC, then click Browse to select your backup file.

– To restore from USB, insert a USB drive that has the backup file into a slot on the front of the *groov* Box. Select Load from USB Flash Drive, then click the browse button and select your backup file.


USB connectors for backing up and restoring

5. Click Restore, and then wait while the files are uploaded.

Updating *groov* Admin

You can update your entire *groov* Admin from an application update file downloaded from the Opto 22 website. All of your configuration settings will be kept.

1. Go to manage.groov.com and follow directions to download and save the *groov* Admin update file to your computer.

2. Click Quick Start and then Update *groov* Admin.
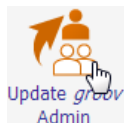
3. Click Browse to locate the *groov* Admin software update file on your computer.

4. Highlight the file, and click Open.
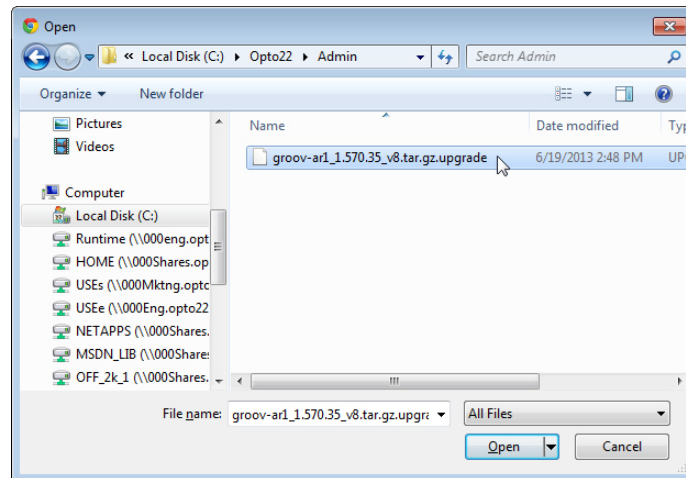
5. Click Update.

The application file is downloaded, and the neccessary components are installed.

6. After the *groov* Box is done updating, click "Click here to restart now."

Your *groov* Box must be restarted for the update to take effect. (Other ways to restart the *groov* Box are described in the next section,)

During the restart, you'll notice the LED lights on the *groov* Box go off and then come back on. While the *groov* Box is restarting you cannot continue working in *groov*. All users will be disconnected. The *groov* applications will automatically restart once the *groov* Box has fully restarted and the SYS LED has stopped flashing.

Restarting the *groov* Box

When the *groov* Box is restarted, all users will be disconnected and you won't be able to continue working in *groov* Build. The *groov* Box must be restarted in order for updates to take effect.

To restart the *groov* Box hardware, do one of the following:

• After updating the *groov* Box, the following message appears. Click "Click here to restart now."

- Select System > Restart *groov* Admin.

- Click System Information, then click "Click here to restart now"
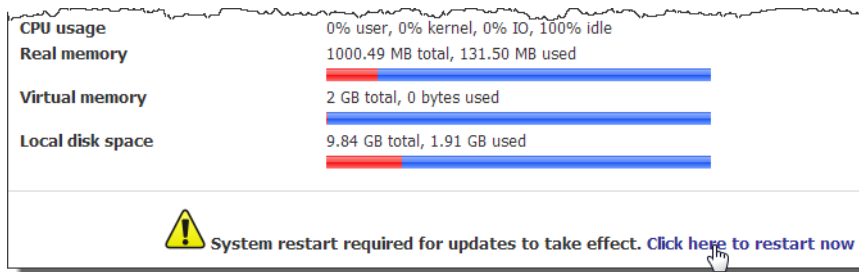
- Press the On/Off button and wait for the *groov* Box the to turn off. Then press the On/Off button again to power it back up.

  During restart, you'll notice the LED lights on the *groov* Box go off and then come back on. While the *groov* Box is restarting you cannot continue working in *groov*. All users will be disconnected. The *groov* applications will automatically restart once the *groov* Box has fully restarted and the SYS LED has stopped flashing.

Changing the Username and Password

You can change the username and the password for the *groov* Admin user that is currently logged in. This does not affect the usernames and passwords in Build.

1. Under System in the menu tree, select Change Username/Password.
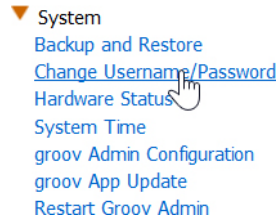
2. Enter the new Username or password in both boxes, and then click Save.

CAUTION: *Write down your Username and Password, and keep it in a safe place. You will need this information each time you log in. If you lose your login information, you will have to restore the groov Box back to factory defaults which will erase your project. There is no password recovery option.*

The login dialog box appears.

3. Log in using the new username and password.

Checking System Information

Select System Information in the menu tree, or click the System Information icon in Quick Start.
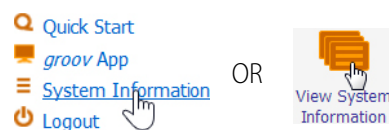
The following information is provided.

OPTO 22

System hostname	opto-00-d2-dc
Activation key	Visit: activate.groov.com to activate your Groov box
groov **Serial Number**	1396322356
groov **Part Number**	GROOV-AR1
groov **Image version**	19
groov **Admin version**	1.570.39
groov **App version**	R2.1d (r21630)	June 12, 2014 2:12 PM
Time on system	Mon Feb 9 20:42:30 2015
System uptime	2 days, 21 hours, 09 minutes
CPU load averages	0.44 (1 min) 0.55 (5 mins) 0.58 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	1000.45 MB total, 132.79 MB used
Virtual memory	2 GB total, 0 bytes used
Local disk space	9.84 GB total, 1.85 GB used

Checking Hardware Status

To check the status of the internal components in *groov* Box, click Hardware Status in the menu tree under System.

▼ System
　Backup and Restore
　Change Username/Password
　Hardware Status
　System Time
　groov Admin Configuration
　groov App Update
　Restart Groov Admin

The following information is provided.

Hardware Status

Help...
Module Config

Internal Temperature 1	35.94 C
Internal Temperature 2	34.00 C
CPU Temperature	34.00 C
Input Voltage	15.12 V
Battery Voltage	3.24 V

If any value is out of range, it will be displayed in red and a message will appear.

- **Internal Temperature 1**—Temperature of the internal PCB

- **Internal Temperature 2**—Temperature of the internal PCB

- **CPU Temperature**—Temperature of the CPU

- **Input Voltage**—Main power supply for *groov*

- **Battery Voltage**—Voltage of the battery that maintains the date and time.

Changing the Hardware Status Temperature Units

You can change the temperature units for Hardware Status.

1. Under System in the menu tree, click Hardware Status.

2. Click Module Config under Help on the right-hand side.

3. Select either Fahrenheit or Celsius, then click Save.

Setting the System Time

You can set the time used by the *groov* Box.

1. Under System in the menu tree, select System Time.

2. Set the time and date and then click Apply.

Changing the Time Zone

The default timezone is set to UTC (Coordinated Universal Time).

1. Under System in the menu tree, select System Time.
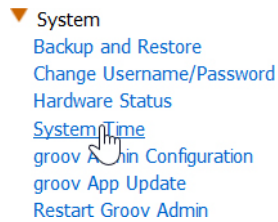
2. Click the Change timezone tab.
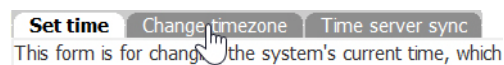
3. In the drop-down list, select a time zone, then click Save.
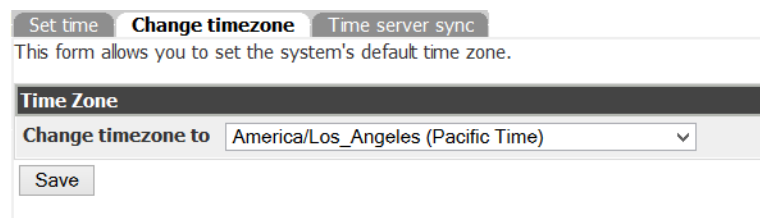
Time Server

Use the Time Server dialog box to configure the system to automatically synchronize the time with a remote server. Synchronization will be done using the Unix time protocol or NTP, depending on what the remote system supports.

1. Under System in the menu tree, select System Time.
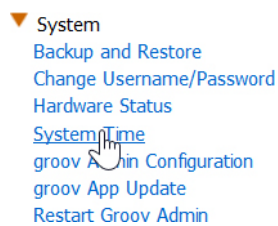
2. Click the Time server sync tab.
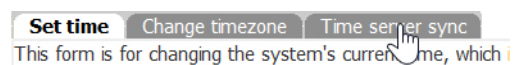
3. Enter the hostnames or addresses of the time servers.

4. Select Yes next to "Synchronize once per day."

5. Click Sync and Apply.

5: Using an SSL Certificate

groov uses an SSL certificate to encrypt communications and prove *groov*'s identity to client browsers. An SSL certificate contains the server name, the name of the organization that controls the server, and digital signatures of organizations that vouch for the authenticity of the certificate. The certificate is digitally signed either by a *certificate authority* (CA) or it is *self-signed*.

The default certificate type (a self-signed certificate) and configuration will cause your web browser to issue an untrusted site warning when accessing *groov*. To avoid the warning you can install the self-signed certificate in all the browser certificate stores used to access *groov*. However, whether or not the certificate is installed in the certificate stores, communication is always encrypted.

Here's a comparison of the certificate types:

	Self-Signed Certificate (default)	Self-Signed Certificate installed on all browser certificate stores	CA-Signed Certificate
Best Use	For one or two *groovs* and a small set of client browsers that remain pretty much the same, and users who trust that your certificate is valid	Same as default, plus it avoids seeing the untrusted site warning from the browser	Use with a system with many *groovs*, or the set of browsers that will access *groovs* is unknown or changes frequently, or users who will not trust your self-signed certificate
Cost	Free	Free	Public CA-signed certificates cost anywhere from $9 to $100 or more per year
Ease of Configuration	Easiest configuration	Must install in the browser certificate store for every browser that accesses the server	More complex initial configuration because a certificate authority signature must be obtained
Untrusted Site Warning	Browser raises untrusted site warning. (But communication is still encrypted.)	No untrusted site warning from browser	No untrusted site warning from browser. Trusted by all major browsers.
Trust Level	Trusted by those to whom the *groov* administrator has demonstrated the validity of the certificate (e.g. by providing the certificate thumbprints).	Trusted by those who trust the *groov* administrator enough to install or let him or her install the certificate in their browser certificate store	Trusted by everyone

If you are using a **self-signed certificate**, see "Using a Self-Signed Certificate" on page 50.

If you are using a **CA-signed certificate**, see "Using a CA-Signed Certificate on groov Box" on page 58.

Using a Self-Signed Certificate

A self-signed certificate encrypts communications, but does not include a digital signature from a commercial CA. It is free and easy to configure, but if you want to avoid having your users see an untrusted site warning every time they use *groov*, you must install the self-signed certificate in the browser certificate store for every browser that will access *groov*. This type of certificate is a good solution for a small set of *groovs* and a small set of client browsers that you can configure.

Follow these steps to create and install a self-signed certificate:

Step 1: Create a Self-Signed Certificate and Private Key

Follow the steps below to generate the following components required to configure self-signed certificate SSL communication. The self-signed certificate is automatically installed on the *groov* Box.

- **Private Key**: This must be kept secret and never shared. Keep a copy of it in a safe and secure place. There is also a **Public Key** included in the signed certificate. You will not handle the public key using *groov* Admin.

- **Signed Certificate**: Contains identification information, the public key, and a digital signature. Identification information includes the server name and the name of the organization that controls the server. The self-signed certificate is digitally signed by the Private Key to establish authenticity. The Certificate is automatically installed on the *groov* Box.

To generate a private key and self-signed certificate:

1. In *groov* Admin, select Networking > SSL Configuration.
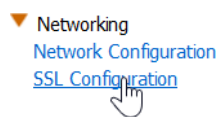
2. Click the Create certificate tab.

3. Fill in the Create SSL key form as follows:

Server name: Enter the fully qualified domain name (or *hostname*) of this *groov* Box that client browsers will use to access *groov*. (See also, "Changing the Hostname, DNS Servers, or IPv4 Gateway" on page 30.) The server name may contain letters a–z (case insensitive), digits 0–9, or a hyphen (-). No other characters are allowed. The server name must not start with a hyphen.

For example, if the URL you will use to access *groov* in client browsers is https://process1.acme.com, then you enter `process1.acme.com`

If you have multiple *groovs* with fully qualified hostnames all with the same domain, another option is to create a self-signed wildcard certificate. For example, if you have two *groovs* with the hostnames *groov1.foo.com* and *groov2.foo.com*, you can create a certificate that has the hostname **.foo.com*. The same private key and certificate are then installed on all the *groovs*.

Server name: Enter the hostname of this *groov* Box that client browsers will use to access *groov*. (See also, "Changing the Hostname, DNS Servers, or IPv4 Gateway" on page 30.) The

server name may contain letters a–z (case insensitive), digits 0–9, or a hyphen (-). No other characters are allowed. The server name must not start with a hyphen.

For example, if the URL client browsers will use to access this *groov* Box is:

https://process1.acme.com, enter `process1.acme.com`

If the URL client browsers will use to access this *groov* Box is:

https://mobilehmi, enter `mobilehmi`

Email address: (optional) Enter the email address of the person responsible for administering this certificate.

Department: Use this field to differentiate between divisions within an organization. For example, you might enter "Engineering" or "Manufacturing." If applicable, you can enter the DBA (doing business as) name in this field.

Organization: The legally registered name of your business. This business must be the legally registered owner of the domain name.

City or Locality: Name of the city or locality where your organization is located. Spell out the name of the city or locality. Do not abbreviate.

State: Full name of the state, province, region, territory where your organization is located. Do not abbreviate.

Country code: The two-letter International Organization for Standardization (ISO-) format country code for the country in which your organization is legally registered. Click here for a complete list of ISO country codes.

RSA key size: Both the public key and the private key. The recommended key size is 2048 bits. Avoid key sizes smaller than 2048 bits.

Days before expiry: Enter the number of days before the self-signed certificate is expired and has to be replaced. It's up to the *groov* Administrator how many days to enter. For example, if you want the certificate to be valid for 10 years, enter 3650.

4. Click Create Now.

groov Admin creates the new private key and self-signed certificate. *groov* Admin also creates a certificate signing request (CSR) to use if you want to obtain a CA-signed certificate (see "Using a CA-Signed Certificate on groov Box" on page 58).

groov Admin displays all of these together.

At this point, the new certificate is installed on the *groov* Box and network services restarts.

5. Copy the **private key** portion of text and paste it to a file named *<server name>-key.pem*
(where *<server name>* is replaced by the server name value you entered on the Create SSL key
form.) This is the private key that was installed on the *groov* Box in the previous step.

*NOTE: Do not lose the private key. You must keep a copy of it to restore later in case you commission a
replacement groov Box or have to restore the Box to factory defaults.*

6. *IMPORTANT: Before proceeding,* wait for the SYS LED on the *groov* Box to stop blinking green,
then make sure to refresh your browser.

It might take some time, but eventually you should see the security warning. (The security warning appears because the new certificate that was just installed on the *groov* Box is not trusted by the browser.)

7. Accept the security warning as described below. For more information, see "Accepting the Security Warning" on page 23.

For Chrome: Click "Proceed anyway."

For Firefox:

– Expand "I Understand the Risks."

– Click Add Exception to open the Add Security Exception dialog box.

– Select "Permanently store this exception."

– Click Confirm Security Exception.

For Internet Explorer 10: Click "Continue to this website (not recommended)."

For Safari: Click Continue.

8. When *groov* Admin returns, select Networking> SSL Configuration.

▼ Networking
  Network Configuration
  SSL Configuration
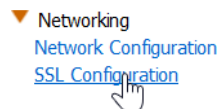
9. Click the Current Certificate tab, then select "PEM format."

Current certificate	Create certificate	Upload certificate

This section shows the details of the current *groov* Admin SSL certificate, and allows it to be downloaded so that it can be accepted by your browser.

Details of current certificate

Authority name	192.168.0.104	**Organization**	OPTO 22 on dscarr-AR1
Issuer name	192.168.0.104	**Issuer organization**	OPTO 22 on dscarr-AR1
Valid until	Feb 4 22:24:06 2045 GMT	**Certificate type**	Self-signed

Download certificate PEM format | PKCS12 format | CSR

The certificate's text appears.

```
-----BEGIN CERTIFICATE-----
MIIEBTCCAu2gAwIBAgIJAMz8yixPBBGyMA0GCSqGSIb3DQEBCwUAMIGYMQswCQYD
VQQGEwJVUzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCFRlbWVjdWxhMSEwHwYDVQQK
DBhPUFRPIDIyIG9uIG9wdG8tMDAtZDItZGMxDDAKBgNVBAsMA0VuZzEWMBQGA1UE
AwwNMTkyLjE2OC4wLjEwNDEgMB4GCSqGSIb3DQEJARYRZHNjYXJyQG9wdHAyMi5j
b20wHhcNMTUwMjEwMjEzNTU3WhcNNDUwMjEwMjEzNTU3WjCBmDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgMAkNBMREwDwYDVQQHDAhUZW1lY3VsYTEhMB8GA1UECgwYT1BU
TyAyMiBvbiBvcHRvLTAwLWQyLWRjMQwwCgYDVQQLDANFbmcxFjAUBgNVBAMMDTE5
Mi4xNjguMC4xMDQxIDAeBgkqhkiG9w0BCQEWEWRzY2FyckBvcHRwMjIuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApGMvd+ATfSBegut+qy0C20QP
HJsphbae+OP1mKl8LRSXGmOkC1+Ul2qMf7vVpokFD2lXmg/ytBOCfcjPuxriGCh5
3RF7mdF4RBaZOTnF7Y3cqdBtQ087UPUfAsv6BXyLXA3qlFMnnsp1+Jrh8l/dNwN/
twIS0rgrDf1j3ugGdV0e4wzZ+SGqoYiIVkASUzV5a3+2SCfojRYxmvvSnfew9Lg4
GWUJMTHW0qmpCwXgBOIasXzyvxxwIO4zqZEygbVhnltjCgSxhnm/86O7s6lRh7Fd
ZtllvEj8X/T/oDceFp7Na48fKUggjo7ubcYEWiAnWpLbA/8LdfW4mDoSok2bhQID
AQABo1AwTjAdBgNVHQ4EFgQUb+2Tvx3Rpg3b9ZB1hwrZiIitutswHwYDVR0jBBgw
FoAUb+2Tvx3Rpg3b9ZB1hwrZiIitutswDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAA7lG7qjadOdWHldBwA0VMu85uHzi+NUDLQDVoyJQ2+TVEOgC4m+x
p2wuf/c4+RAvTOeNzxYGvt2iVCmH1vyZWW0VJ3OIXSfgdgkLjN7xioYW5Sjttq0G
g4xGAsN1opxG4Nut9ubjYLSjibF7liGZu4d5/PLhQDHqAUIWHk+sHyQDiWASgeh0
Spft39SKnNgBLBASwRCnmasqylTYwh1D9AHWXAZVI3hOxCv1qxhKhjRKRWA5bqrG
c5fm0eXf3cGe/XYaDn9iWdt/7fHnJZ7ACncXQVXxjTdF8lZ2Ca9ge2y4E/+ox0Yj
Cg8O1mjL70Bjs96jP9YbWJO+BOGbkhOTjw==
-----END CERTIFICATE-----
```

10. Copy the certificate text and paste it to a file named *<server name>.cer* (where *<server name>* is replaced by the server name value you entered on the Create SSL key form.)

Step 2: Add the Self-Signed Certificate to a Browser Trust Store on a Computer

To prevent the untrusted site warning in browsers, the self-signed certificate must be added to the trust store for each browser used to access *groov*. This section describes how to add a self-signed certificate on a computer. Step 3 describes how add a self-signed certificate on a mobile device.

See the section below for the client computer's operating system.

Windows

Internet Explorer & Chrome

1. In Windows file explorer, locate the *<server name>.cer* file you created in the previous step.

2. Right-click on the file and choose Install Certificate.

The Certificate Import Wizard appears.

Windows 7   Windows 8
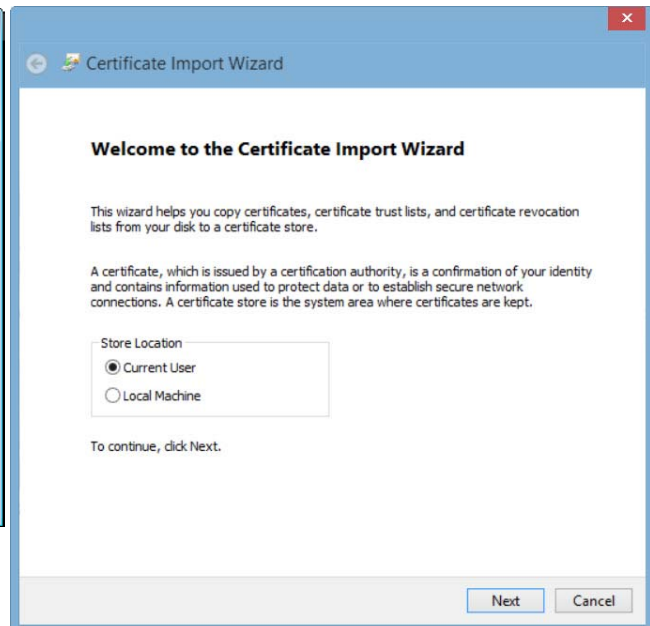
3. (*Windows 8 only*) If you are administrator of local machine, choose the Local Machine certificate store so this certificate will be trusted by all user accounts. Otherwise it will only be trusted by the current user account.

4. Click Next.

5. Select "Place all certificates in the following store."

6. Click Browse to open the Select Certificate Store dialog box.

7. Select Trusted Root Certification Authorities, and then click OK.

8. Click Next.

9. Click Finish.

10. A security warning alerts you that certificate installation is a risk if you don't trust the certificate.

11. Click Yes to affirm that you trust the self-signed certificate.

12. To verify the certificate was installed correctly, open Internet Explorer or Chrome and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Firefox

The self-signed certificate is added to the certificate store by adding a security exception. Firefox will present several warnings about creating a security exception for a self-signed certificate, but because you created and control the private key and certificate and installed the private key on the server, you can trust the certificate identifies your server.

1. Open Firefox and enter `https://<server name>`

   A warning appears that says, "This Connection is Untrusted."

2. Expand "I Understand the Risks."

3. Click Add Exception to open the Add Security Exception dialog box.

4. Select "Permanently store this exception."

5. Click Confirm Security Exception.

Expand this ———— I Understand the Risks

Click here ———— Add Exception...

Click here ———— Confirm Security Exception
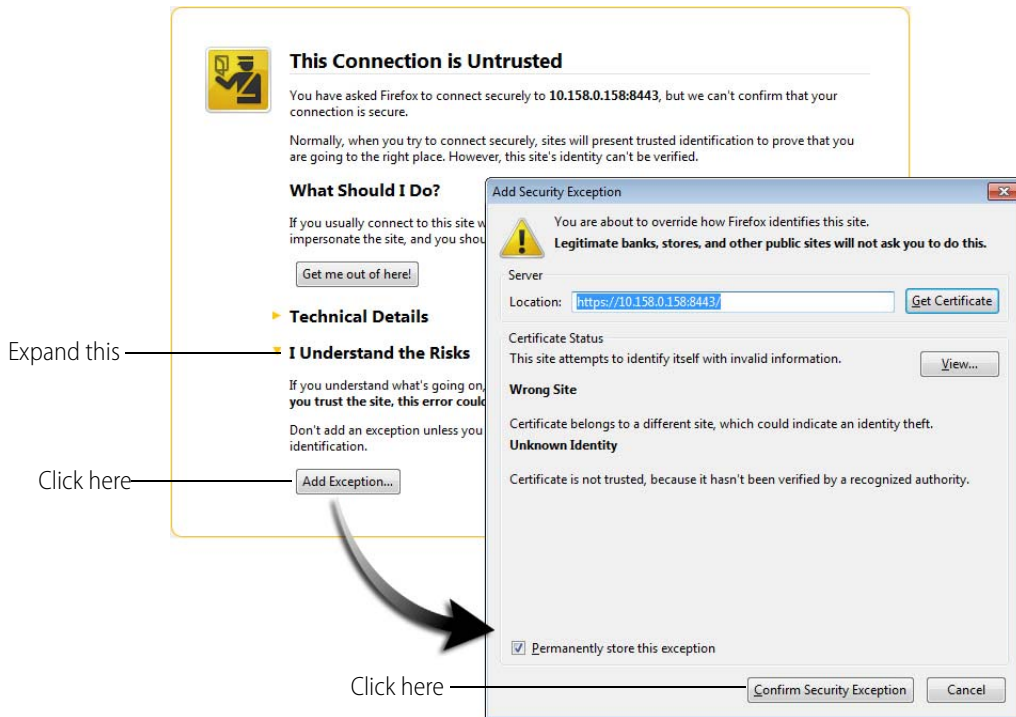
6. To verify the certificate was installed correctly, open Firefox and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

OS X

Safari and Chrome

1. Open Safari and enter https://<server name> to open this dialog box:

2. Click Show Certificate to reveal the full details:
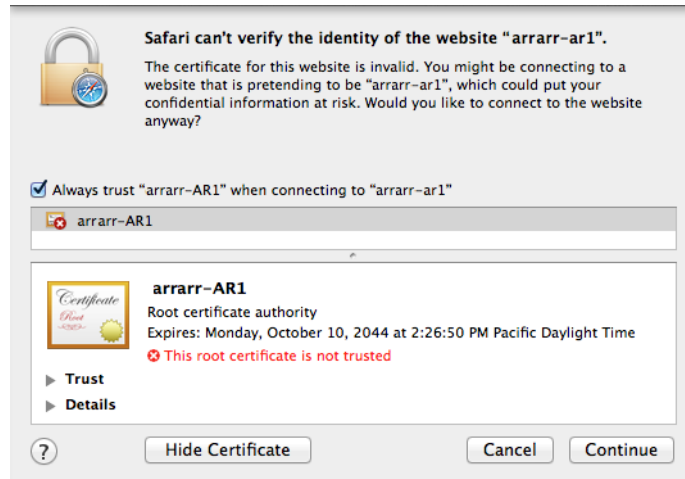
3. If the certificate looks good to you, check the "Always trust *<server name>* when connecting to *<server name>*" and click Continue. You will be asked to provide your password to authorize the addition of this certificate to your keychain, after which the browser and the Hosted Projects window will accept the SSL certificate as valid.

4. To verify the certificate was installed correctly, open a browser and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Step 3: Install an SSL Certificate on Mobile Devices

When you open the operator interface in a browser on a smart phone or tablet a security warning will appear unless you have installed a self-signed SSL certificate. See the section below for the device's operating system.

-
-

iOS Devices

1. Email the *<server name>.cer* file you created previously (see) to an email account accessible from iOS.

2. On the iOS device, open the email message containing *<server name>.cer*.

3. Tap on *<server name>.cer*

4. A message appears, "The authenticity of *<server name>* cannot be verified..."

5. Click Install.

6. Click Install Now.

7. Click Done.

8. To verify the certificate was installed correctly, open a browser and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Android Devices

1. Email the *<server name>.cer* file you created previously (see "Step 1: Create a Self-Signed Certificate and Private Key" on page 50) to an email account accessible from Android.

2. On the Android device, open the email and click the *<server name>.cer* file to install the certificate.

3. When prompted for a certificate name, type in a name. Make sure "Credential use:" is set to "VPN and apps."
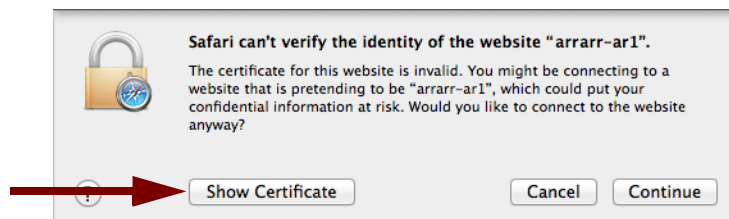
4. Click OK.

5. To verify the certificate was installed correctly, open a browser and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Using a CA-Signed Certificate on *groov* Box

Follow these steps to create a certificate signing request (CSR) and install a CA-signed certificate:

"Step 1: Create a CSR" (see page 58)

"Step 2: Obtain a CA-Signed Certificate" (see page 60)

"Step 3: Install the CA-Signed Certificate on groov Box" (see page 61)

Step 1: Create a CSR

IMPORTANT: This procedure will create and install a new private key on the groov box.

Follow the steps below to generate a certificate signing request (CSR).

You will send the CSR to the Certificate Authority (CA) of your choice. The CA verifies the identification information and signs the CSR, which then becomes a CA-signed Certificate.
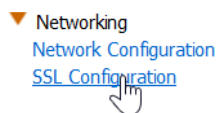
1. In *groov* Admin, select Networking > SSL Configuration.

▼ Networking
  Network Configuration
  SSL Configuration

2. Click the Create certificate tab.

3. Fill in the Create SSL key form as follows:

   Server name: Enter the fully qualified hostname of this *groov* Box that client browsers will use to access *groov* (i.e. the hostname and domain name, such as *mobilehmi.mydomain.com*.) The server name may contain letters a–z (case insensitive), digits 0–9, or a hyphen (-). No other characters are allowed. The server name must not start with a hyphen.

   For example, if the URL you will use to access *groov* in client browsers is https://process1.acme.com, then you enter `process1.acme.com`

   If the URL client browsers will use to access this *groov* Box is:

   https://mobilehmi.mydomain.com, enter `mobilehmi.mydomain.com`

See also, "Changing the Hostname, DNS Servers, or IPv4 Gateway" on page 30.

Email address: (optional) Enter the email address of the person responsible for administering this certificate.

Department: Use this field to differentiate between divisions within an organization. For example, you might enter "Engineering" or "Manufacturing." If applicable, you can enter the DBA (doing business as) name in this field.

Organization: The legally registered name of your business. This business must be the legally registered owner of the domain name.

City or Locality: Name of the city/locality in which your organization is registered/located. Spell out the name of the city/locality. Do not abbreviate.

State: Full name of the state, province, region, territory where your organization is located. Do not abbreviate.

Country code: The two-letter International Organization for Standardization (ISO-) format country code for the country in which your organization is legally registered. Click here for a complete list of ISO country codes.

RSA key size: Both the public key and the private key. The recommended key size is 2048 bits. Avoid key sizes smaller than 2048 bits.
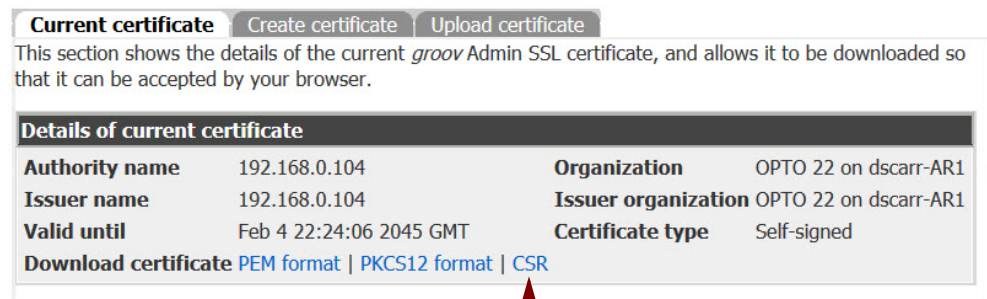
Days before expiry: This does not affect a CA-signed certificate, so you can leave this blank.

4. Click Create Now.

groov Admin creates a certificate signing request in addition to a new private key and self-signed certificate (which is automatically installed).

groov Admin initially displays all of these together.

5. Select the Current Certificate tab, then click the CSR hyperlink at the bottom of the dialog box.

Current certificate	Create certificate	Upload certificate

This section shows the details of the current *groov* Admin SSL certificate, and allows it to be downloaded so that it can be accepted by your browser.

Details of current certificate

Authority name	192.168.0.104	Organization	OPTO 22 on dscarr-AR1
Issuer name	192.168.0.104	Issuer organization	OPTO 22 on dscarr-AR1
Valid until	Feb 4 22:24:06 2045 GMT	Certificate type	Self-signed

Download certificate PEM format | PKCS12 format | CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3jCCAcYCAQAwgZgxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTERMA8GA1UE
BwwIVGVtZWN1bGExITAfBgNVBAoMGE9QVE8gMjIgb24gb3By0wMC1kMi1kYzEM
MAoGA1UECwwDRW5nMRYwFAYDVQQDDA0xOTIuMTY4LjAuMTA0MSAwHgYJKoZIhvcN
AQkBFhFkc2NhcnJAb3B0cDIyLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANWp3jKqPrlMtZFX0c5bJ3WiBt9ZifLe2cMgr7xg3z0pTEeKPfIqst32
hvJnsIyCr45C6rMCQVbiV9vxtaLHBN39DItS7gO6WrNq9kbYnUnkSVwE/fr8toPk
MdzVxmIt877A3ZtcEI3YxnFLSxsNcGOD4BFajoynNWlHMDN5Qnxyfv034czvLM/E
kKbfo/zZAJjMCWrBefEUfNxDwOsf2cfreFtbMyeB1oOqy65bB3RRSxRC2lBOAMIi
bi+eRIAVmIf8YrpgijyPRdJOpnBVNfe8GlR6qhl3SXPwuVBorCvl8UXCqHwQtgOJ
YHanWnzsaBPTVfqLmzHcO0DbdbiV+LUCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IB
AQDBvZEJPcUlpm03hmQZekQp3OLIUwFl20ctXZK3GNzUaqo0Rv92emV4HW3TrYlw
iYrbe+bsaBDg4DN93sF6bEwr6ryKBCvGuBIES5nLgZsm1+DeAat1kLFwVWqTBhwg
BY032tiiBn/j8E+hx0M5zg8nIHPS8OPQ1RkyTbABu7Tmmj8Q7WmymdgdZcCT+rpn
FS99Xfepkq/s7YrCs3b2iMj35UMTZtimyg13fQ2I56byMcbZLQ69Baq8qwYpvooi
N0HQXUdTQNwXi+pdDnGpSxsmb5UnZ2kDcF7cHvDCrFBBpFGruXA0ER5Ik0ZixMBB
d3Xoxd/9VxOtja7u0Q/xvwxJ
-----END CERTIFICATE REQUEST-----
```

6. Copy and paste the entire text to a file named *<server name>.csr* (where *<server name>* is replaced by the server name value you entered on the Create SSL key form in step 3.)

Step 2: Obtain a CA-Signed Certificate

A CA-signed certificate contains identification information, the public key, and a digital signature. Identification information includes the server name and the name of the organization that controls the server. The certificate is digitally signed by a CA to establish authenticity. The Certificate is installed on the *groov* Box or Server.

When you apply for an SSL certificate from a certificate authority, you will need to send them the information captured in a Certificate Signing Request (CSR). If you have not yet created a CSR file, see "Step 1: Create a CSR" on page 58.

When filling out a form for a certificate authority, keep in mind that an SSL certificate can be used with any operating system. If you are asked to select an operating system, you can select "other" if that is an option, but it's OK to select some other operating system.

1. Open the .csr file you created previously in "Step 1: Create a CSR" on page 58.

2. Provide the text of the CSR to the certificate authority in whatever form they require, whether it's a text file or just text pasted into a text field.

To paste the text into a text field on the CA's website, open your .csr file in a text editor such as Notepad, select all of the text and press CTRL+C to copy the text to the clipboard.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICjTCCAXUCAQAwSDELMAkGA1UEBhMCdXMxITAfBgNVBAoMGE9QVE8gMjIgb24g
b3B0by0wMi0yYS1hNjEWMBQGA1UEAwwNb3B0by0wMi0yYS1hNjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAPnEPMiUKONk5YKpt4jwtl83qShIKHpPOIbE
c3D4IpSa0e1iPjbyIxsesY68DmqcXEvPXzSxyjeFVHKgDdOgrQIVhrAtUWn4aLCU
sNI9GbcCOft1dLRxxceyIlDeVQD5KI6DR2xCGnqvMwpc8tzbJksYWroPjCRFwVi7
V5oG405YGsqxBQAVKiQBRyjTJUkKDu/HGb5WtVYUoieoguLlnhnttpH71Kk2iZ+K
ZgXss8WO17v9/I4nsc9sFTq8Iclg9G9tSfSjX+S46UfVmeu2ExYzbz3dvTJF6mzC
z9mL5Q5Sy6RZT56ksJGMZGVaQo9sfHcgjdYJIbAEpM9nYXfDgq8CAwEAAaAAMA0G
CSqGSIb3DQEBBQUAA4IBAQCvRm0AQVeMyj6LC7YBLCP5iGnlFM++PH3rZjwrJi2b
rOdgStAeYLMewo+XU/8G5pMojnwhfvBnBbukovA7gi77my0JBvQPLJBQ8u9GQlEU
GY7r19gcn9uncW6FzkH0WNkvCC6Ps5lqPUgcBQE9+/aI10MRWNdwVLVZn21HKYMH
+H/SdPFtbSUzoHvHBJNZG5WPaJwrdrnOSvdLtOuPl/TBuOKIDTmqjYoUANtyjQnc
U745b/kU8RQuNsyvk6aFmNP7oWgIou7CgWQ09ZfFcEGATn3+QDXHl5tlpYOGLjMM
7UD2Y6uE9s5sxv2ME6V2BAP6Vk8DcSWDq78NhQcwkj/X
-----END CERTIFICATE REQUEST-----
```

3. Finish the transaction with the certificate authority and receive your new SSL certificate.

Step 3: Install the CA-Signed Certificate on *groov* Box

1. In *groov* Admin, select Networking > SSL Configuration, then click SSL Encryption.
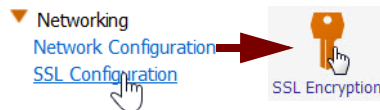
2. Click the Upload certificate tab on the SSL Encryption page.

3. Under "Private key text" click Browse and specify the *<server name>.key* file created previously. See "Step 1: Create a Self-Signed Certificate and Private Key" on page 50.

NOTE: The Private Key should be kept private. If it gets compromised, security is no longer guaranteed.

4. Under "Certificate text" click "Entered below," then click Browse and specify the file containing the signed certificate that was obtained from the CA.

5. If your CA used intermediate CA certificates, they should all be contained in a single file. (If you are not sure if your CA used intermediate CA certificates, ask your CA.)

For example, if you obtained your signed certificate from StartSSL™, the certificate was downloaded to a file named *sub.class1.server.ca.pem*.

    a. Under "Chained certificate text," select "Entered below."

    b. Click Browse and specify the file containing all the intermediate CA certificates in the certificate chain between your certificate and the root CA certificate. For a StartSSL class 1 free certificate this is *sub.class1.server.ca.pem*.

6. Click Save to complete the process.

The browser pauses for a few seconds while the certificates are applied to the *groov* box. When the certificates have been installed successfully, a confirmation message appears.

7. To verify the certificate was installed correctly, use a browser to access the *groov* Box using the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

6: Troubleshooting and Q&A

Basic Troubleshooting

The *groov* Box is not receiving power

- Make sure you are using either the power supply that came with *groov* Box or else a power supply with the appropriate specifications. See "Appendix A: Specifications and Dimensions" on page 67.

- Check that the power supply is securely attached to the *groov* Box and the power supply is receiving power.

The *groov* Box is connected to the Ethernet network, but nothing is working

- Make sure the *groov* Box has been turned on, and the LNK ACT LED for the connected Ethernet interfaces are lit. (See "LEDs" on page 70.)

- Make sure you've typed the URL accurately and included the "s": https:// plus the *groov* Box hostname or IP address. Check the label on the bottom of the *groov* Box, where the hostname should be written.

  URL examples:

  – https://opto-06-51-f2

  – https://192.168.11.2

- If you cannot connect to *groov* on the network, make sure the Ethernet cable is connected to ETH0, which must be used for initial setup and configuration. After that, either ETH0 or ETH1 may be used.

- Make sure that the *groov* Box and the computer are connected to the same network. If you still can't reach the Box, your network is set up differently. That's OK. Find out the following information about your network and your computer:

  – Does your network have a DHCP server?

  – Does your network have a DNS server?

  – Does your computer have more than one network interface card (NIC)?

See the next questions for more answers.

Troubleshooting Q&A

Q: What's a DHCP (dynamic host configuration protocol) server?

A: A DHCP server automatically assigns IP addresses to devices on the network, which is what the *groov* Box expects. If you have no DHCP, work with your IT Department to choose a static IPv4 address for the *groov* Box. To assign the fixed IP address, you'll need:

- a Windows PC on the same network subnet as the *groov* Box

- *groov* Find utility (on the CD that came with the *groov* Box)

- to assign the static IP address to the Box. See "Assigning a Static IP Address" on page 29.

Once you've assigned the static IP address, open your web browser and for the URL enter https:// plus the IP address you assigned to *groov*. For example: https://182.154.1.68

Q: What's a DNS and what if I don't have one?

A: A DNS (domain name server) keeps track of the unique hostname for each device on the network, so you can find it by name even if its IP address changes. If your network has no DNS, you won't be able to access the *groov* Box using its hostname, but you can access it using its IP address.

To determine the IP address, you'll need:

- a Windows PC on the same network subnet as the *groov* Box

- *groov* Find utility (on the CD that came with the *groov* Box). See "To open groov Admin using groov Find (Windows only)" on page 21.

Once you've found your *groov* Box in *groov* Find, click the link to set up the Box. Also make a note of the IP address shown, so later you can use it in your web browser instead of the hostname: for the URL enter https:// plus the Box's IP address. For example: https://192.168.1.220

Q: My computer has more than one NIC. What does that mean?

A: More than one NIC can cause a problem when you're trying to communicate with *groov* using your browser and the *groov* Box's hostname.

Each NIC communicates on a separate network subnet. You may have one network subnet set up for your computers and a second one set up for your control system, for example (this is a pretty common scenario, and in fact we recommend it for security).

Make sure you're trying to reach the *groov* Box using the NIC for the network subnet it is on. You could unplug the Ethernet cable from your controller network NIC to force the PC to look for the *groov* Box on the computer network. Then try again using your browser and the *groov* Box's hostname.

If your control system and your computers are on separate network subnets, you'll need to set up ETH1 on the *groov* Box in order to reach your control system. See the next question.

Q: When I try to configure the Modbus/TCP device, OPC UA server, or Opto 22 SNAP PAC controller, it can't be found.

A: Are your control system and your computers on separate network subnets? We recommend this setup for security reasons, and the *groov* Box is designed to work this way. Here's what to do so *groov* can find your OPC UA server, Opto 22 SNAP PAC controller, or Modbus/TCP device:

1. Plug the control network into ETH1 on the *groov* Box. (Remember, your computer network is plugged into ETH0. The two Ethernet network interfaces on the Box are independent, so that keeps the two network subnets separate.)

2. Follow the steps in "Configuring ETH1 for the Control Network" on page 31 to configure the ETH1 connection.

3. Now try configuring your tag server or controller again. This time *groov* should be able to find it.

Q: I can't log into *groov* using the hostname. What should I do?

When starting a *groov* Box, always wait until the SYS LED has stopped blinking before you try to access *groov*. Otherwise, you might not be able to log in using the hostname. If this happens, try one of the following methods to log in:

Method 1: Open *groov* Find and locate the IP address of the *groov* you want to log into. Log into *groov* using the IP address. After some time passes, you should be able to log in again using the hostname.

Method 2: Open a command prompt and enter `ipconfig /flushdns`. Then log into *groov* using the hostname.

Q: I can't read (or write) to my Modbus/TCP device OR the data doesn't make sense. What's wrong?

Modbus/TCP devices, though based on a standard protocol, may be set up differently from one another. Some use zero-based addressing and some use one-based addressing. Some devices don't support all Modbus functions. Modbus/TCP devices also vary in the way they present float data. And device documentation sometimes doesn't specify how the device is set up.

If you're having trouble reading or writing to your device, or if the data is clearly wrong, you probably need to change settings for your Modbus device. In groov Build, choose Configure > Devices and Tags and locate your device in the list. Follow instructions in the *groov Build and View User's Guide* to understand and change settings. You may need to try different combinations of settings to see what works.

Additional Questions and Answers

This section answers questions you might have about the *groov* Box.

Q: Where should I locate the *groov* Box?

A: The *groov* Box is an industrial appliance made to operate in tough environments, so it doesn't have to be pampered. Make sure you check the specs for temperature and humidity, and then place it where you can connect it to both your company computer network and your control network. (You will use separate connectors on the *groov* Box for these two networks to keep them physically separated—better for security.)

If you're using the wireless LAN, choose a location where the signal is constant and strong. Wireless networks can be unreliable unless carefully designed and periodically checked.

The Box can be mounted on a DIN rail or on a wall or equipment using one of the mounting brackets provided. Make sure there's space on both sides of the box so air can flow freely around the device.

If you're a machine builder or OEM and including *groov* in your machine, the same basic ideas apply: check specs, check security, and mount where there's room for the Box to breathe. Also, make sure you have network access to the Box for updates.

Q: How do I connect the *groov* Box?

A: Plug the *groov* Box into your Ethernet computer network using the ETH0 connector. You must use ETH0 because that's the network interface the *groov* Box uses to send a DHCP request—which is how it gets an IP address so your network knows where it is.

Next, plug the *groov* Box into your Ethernet-based control network using the ETH1.

Now plug the power supply into the *groov* Box and into a standard 120 or 240 VAC wall outlet. The power supply handles 100–240 VAC, so if you're outside North America, just use an adapter plug.

Once it's plugged in, firmly push the On/Off button to turn it on.

See Chapter 2: Getting Started.

Q: What's the function of the USB ports on the *groov* Box?

A: The USB port on the top is for a USB WiFi adapter for connecting to a wireless network (see "Configuring Wireless Communications" on page 32). The USB ports on the front are for using a USB flash drive for backing up and restoring project components (see "Backing Up groov" on page 37 and "Restoring groov" on page 39).

Q: What happens if power is removed from a *groov* Box and then restored?

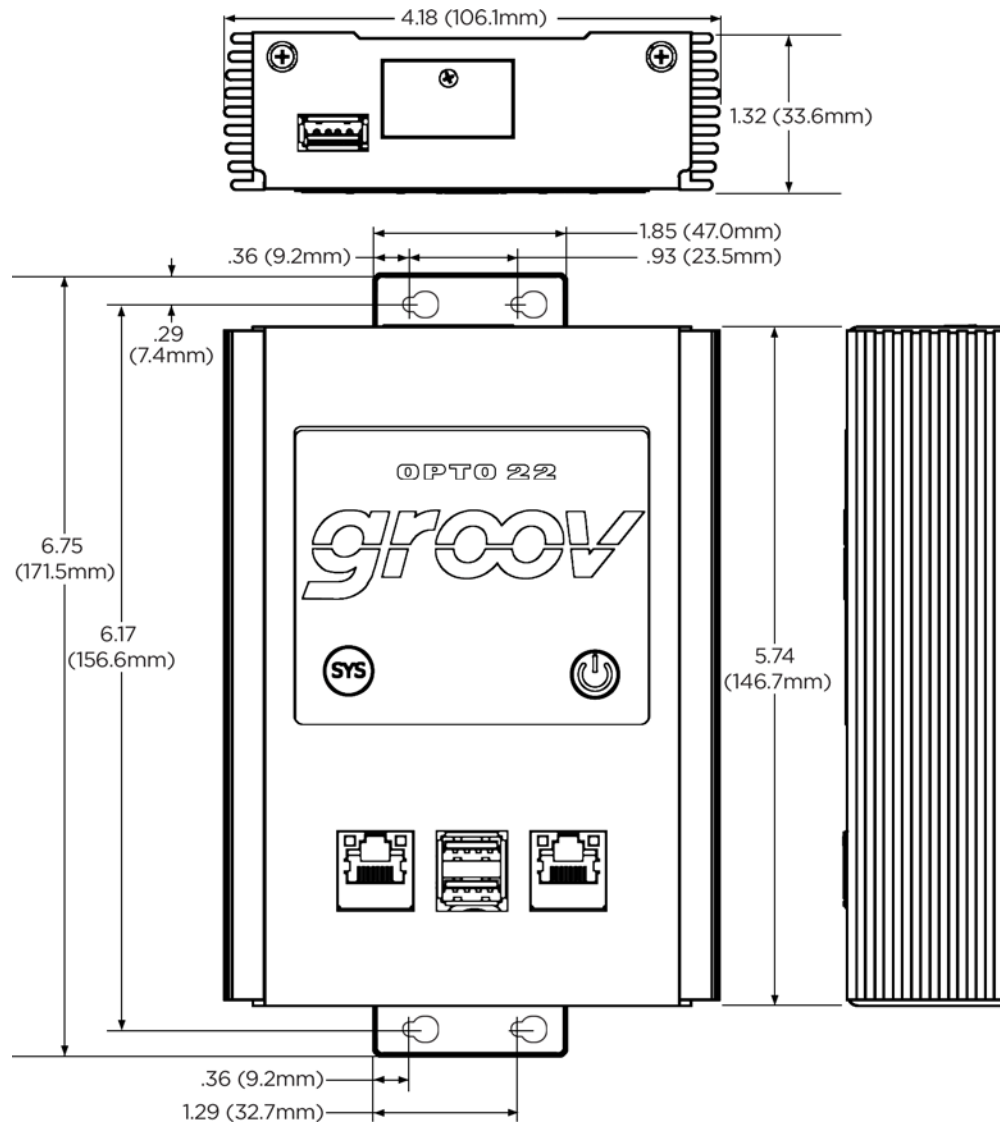If power to the groov box is removed, such as when there is a power outage, when the power is restored the *groov* box will return to the state it was in prior to the power being removed. If it was on, it will power up. If off, it will remain off.

A: Specifications and Dimensions

Specifications

Ethernet Communication (wired)	Two independent 10/100/1000 Mbps RJ-45 connectors, each with a separate IP address (separate subnets)
Ethernet Comm (wireless)	(Optional) 802.11 b/g/n provided by a commercial USB WiFi adapter that has been tested and approved by Opto 22
Security (wireless)	WEP64 WEP128 WPA PSK (also known as WPA Personal) WPA2 PSK (also known as WPA2 Personal)
Backup battery	BR2032 button cell lithium battery with a nominal voltage of 2.8 volts. Lasts 8 years at 25 °C. This battery maintains the date and time.
Power Consumption	8-36 VDC, 24 VDC @ 500mA (Power supply included; input 100-240 VAC. Use international adapter if needed.)
Enclosure	Compact and sturdy metal. Fanless operation.
USB	USB 2.0 (three)
Indicators	Ethernet interfaces (2): Link/Activity and Speed System: SYS & PWR
Operating Temperature	0 to 70 °C (32 to 158° F)
Storage Temperature	-20 to +80 °C (-4 to 176° F)
Operating Humidity	10% to 90% relative humidity, non-condensing
Storage Humidity	5% to 95% relative humidity, non-condensing
Agency Approvals	CE, RoHS, DFARS
Warranty	30 months

Dimensions

B: Connectors and LEDs

Connectors and Indicators

USB connectors for
backing up and restoring

Independent 10/100/1000 Mbps
Ethernet interfaces (RJ-45 connectors)

Top

Bottom

USB connector for
WiFi adapter*

Power connector

* For more information, see

LEDs

The *groov* Box's LEDs use color and blinking to show status information.

| LED	What it shows	Color	What it means
SYS	*groov* Box status	Off	*groov* Box is turned off
		Green	*groov* Box is turned on
		Blinking green	*groov* Box is booting up
		Blinking blue	*groov* Box is shutting down
		Blinking red and green	Default settings are being restored
		Blinking red	Restoration to default settings failed
On/Off	Power to Box	Green	*groov* Box is turned on
		Blinking red	Input power is outside normal range or battery is low
SPEED	Ethernet link speed	Off	10 Mbps
		Green	100 Mbps
		Orange	1000 Mbps
LINK ACT	Ethernet network activity	Off	No Ethernet link
		Green	There is an Ethernet link, but no activity
		Blinking green	There is a link and activity

C: Replacing the Battery

The battery maintains the Date and Time. If the power LED blinks red, input power is outside normal range or the battery is low and should be checked.
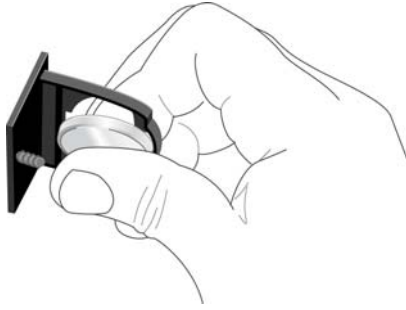

Check the battery if the power LED blinks red.

1. On the top of the *groov* Box, unscrew the captive screw, and pull out the battery holder.
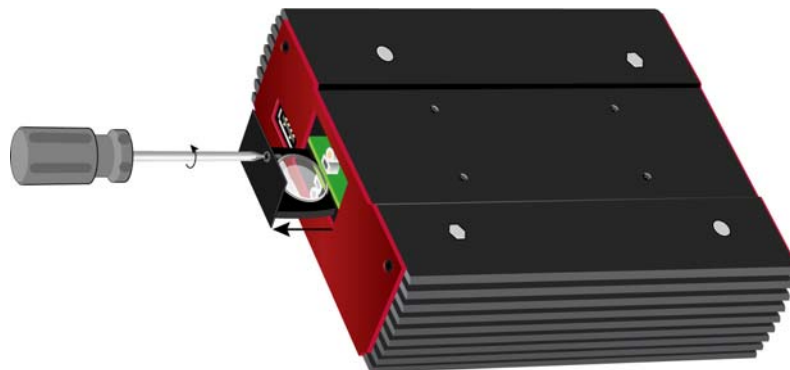
2. Using your fingers, pop out the old battery.

3. Put in a new battery, push in the holder, and secure the captive screw.

D: Installing an Approved USB WiFi Adapter

If you want to use the *groov* Box on a wireless network, you must purchase and install one of the following USB WiFi adapters Opto 22 has tested and approved for use with GROOV-AR1. Unapproved WiFi adapters should not be used.

- Netis WF2119S
- Netis WF2116
- Rosewill RNX-N150UBE
- Patriot Memory PCUSBW1150

Install the WiFi adapter and restart the *groov* Box as follows:

1. If the *groov* Box is on, press the On/Off button to turn it off.

   CAUTION: If you press the button for longer than eight seconds, the groov Box will be restored to default settings. Your project and all passwords will be erased.

2. Insert the WiFi adapter into the USB connector on the top of the device.

Top

USB connector for
WiFi adapter

3. Firmly press the On/Off button. The Power LED will turn on. Wait until the SYS LED has stopped blinking and is solid green.
4. Open *groov* Admin as described on page 20.
5. Configure wireless communications as described on page 32.

Index

A

access point, wireless, 32
architecture, system, 5

B

back up
    groov, 37
browsers, 4, 9, 15, 23

C

CCMP, 33
Chrome, 4, 24
Client Options dialog, 31
communications, 4
control network, 5
CSS3, 4

D

default network settings, 20
DHCP, 20, 28, 64
DIN rail clip, 12
DNS, 15, 28, 64
    servers, 31

E

encryption, 33
enterprise network, 5
environmental requirements, 67
Ethernet connectors, 4, 12, 20

F

Find, 16

Firefox, 4, 24

G

groov Admin
    update, 28
groov Find, 16, 21

H

hardware status, 44
HDTV, 4
help
    Opto 22 Product Support, 7
    Product Support, 7
hostname
    groov Box
        changing, 31
HTML5, 4

I

Internet Explorer, 25
IPv4 Gateway, 31

L

LED
    PWR, 20
    SYS, 20

M

memory, 67

N

network
    configure, 28
    control, 5
    enterprise, 5
    interface card (NIC), 63
    key, 33

O

On/Off button, 19
operating temperature, 67
Opto 22 Product Support
    contacting, 7

P

password
    groov Admin, 42
power
    requirements, 13, 67
private key, 62
processor, 67
PWR LED, 20

Q

quick start, Admin, 28

R

reset groov Box, 20
restart groov Box, 41
restore groov, 39

S

Safari, 25
security
    warning, 16, 23
session timer, 23
SoftAP, 35
specifications, 67
SSID, 33

SSL

SSL
    certificate
        buy, 60
static IP address, 16
    assign, 29
storage temperature, 67
SVG, 4
SYS LED, 20
system
    architecture, 5
    information, 28, 43
    time, 45

T

Technical Support. *See* Opto 22 Product Support, 7
temperature, 45
    and humidity, 67
time
    server, 46
    zone, 46
TKIP, 33
troubleshooting
    Opto 22 Product Support, 7

U

update
    groov Admin, 40
    groov App, 36
USB flash drive
    back up to, 37
    restore from, 39
User Account Control, 21

W

WEP, 33
wired network, 4
wireless
    communications, 32
    LAN, 4
        specifications, 67
WPA, 33